

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2003 年 7 月 24 日 (24.07.2003)

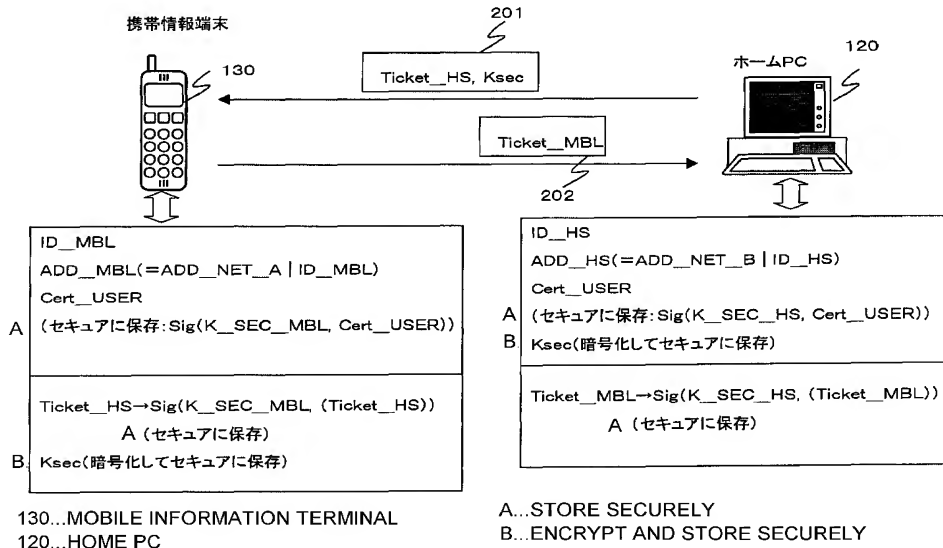
PCT

(10) 国際公開番号
WO 03/061189 A1

- (51) 国際特許分類: H04L 9/08, 9/32, (TAKI,Ryuta) [JP/JP]; 〒141-0001 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
G06F 12/14, 15/00, 13/00
- (21) 国際出願番号: PCT/JP03/00107 (74) 代理人: 宮田 正昭, 外(MIYATA,Masaaki et al.); 〒104-0041 東京都 中央区 新富一丁目 1 番 7 号 銀座 ティーケイビル 6 階 澤田・宮田・山田特許事務所 Tokyo (JP).
- (22) 国際出願日: 2003 年 1 月 9 日 (09.01.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2002-7656 2002 年 1 月 16 日 (16.01.2002) JP (81) 指定国 (国内): CN, KR, US.
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川 6 丁目 7 番 3 5 号 Tokyo (JP). 添付公開書類: — 国際調査報告書
- (72) 発明者; および (75) 発明者/出願人 (米国についてのみ): 瀧 隆太
- 2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: CONTENT DELIVERY SYSTEM

(54) 発明の名称: コンテンツ配信システム



(57) Abstract: A system is realized that allows a secure processing even when an apparatus that requests a download is not the terminal apparatus that is the destination of the download. A content delivery server receives the signature ticket of a download designation from a content download requesting terminal, and verifies the ticket to confirm that the apparatus of the download destination is an apparatus approved by the download requesting terminal, thereby confirming the correctness of the device of the download destination without establishing a direct authentication therewith. A content signature key (Ksig) or hash value is transmitted/received as data that can be cryptographic-processed only at the download requesting and destination apparatuses, and a tampering check of the contents and the like can be executed only at the correct download destination apparatus.

[続葉有]



WO 03/061189 A1



(57) 要約:

ダウンロード要求とダウンロード先端末を異なる装置とした場合のセキュアな処理を可能としたシステムを実現する。コンテンツ配信サーバは、コンテンツダウンロード要求端末からダウンロード先の署名チケットを受信して、チケットを検証してダウンロード先の装置が、ダウンロード要求端末の承認した装置であることを確認して、ダウンロード先機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認を行なう。また、コンテンツ署名用鍵 [K s i g] またはハッシュ値を、ダウンロード要求および先の装置においてのみ暗号処理可能なデータとして送受信し、コンテンツの改竄チェック等を正当なダウンロード先装置においてのみ実行可能とした。

明 細 書

コンテンツ配信システム

5

技術分野

本発明は、コンテンツ配信システム、コンテンツ配信方法、および情報処理装置、並びにコンピュータ・プログラムに関し、特に、コンテンツのユーザ機器に対する送信、ダウンロード処理をセキュアに実行し、かつ利便性を高めたコンテンツ配信システム、コンテンツ配信方法、および情報処理装置、並びにコンピュータ・プログラムに関する。

背景技術

15 昨今、画像データ、音声データ、ゲームプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワークを介してデータ配信サーバからユーザの機器、例えばP C、あるいは携帯機器としてのモバイルコンピュータ、P D A、携帯電話等に送信し、各機器の記憶媒体にデータをダウンロードするといった携帯でのコンテンツの利用が広く普及してきている。

20 P C、携帯端末等の情報機器には、コンテンツをネットワークから受信するためのインタフェースを有し、さらにコンテンツの再生に必要な制御手段、プログラム、データのメモリ領域として使用されるR A M、R O M等を有する。

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、インターネット等を介してユーザ機器内のハードディスク、フラッシュメモリ等の記憶媒体に格納され、コンテンツ再生機器として利用されるP C、携帯端末等の情報機器に対するユーザ指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

コンテンツ配布、すなわち、コンテンツ配信サーバからユーザ機器に対するコンテンツのダウンロード実行に際しては、ユーザ機器が正当なコンテンツ利用許

可を得られたものであるかの認証、例えば公開鍵暗号方式、あるいは共通鍵暗号方式等の各種の認証処理を行なって、ユーザ機器の正当性を確認する処理が行なわれることが多い。

5 昨今の様々な情報処理端末の普及に伴い、個人ユーザであっても自宅にはP Cを有し、屋外では、携帯電話、モバイルコンピュータ、P D A等の携帯機器を使用するといったように、複数の情報機器の利用が一般的になっており、このような各種の機器から、コンテンツ配信サーバに対して様々なコンテンツのダウンロードを要求することが可能になっている。

10 認証を条件としたコンテンツ・ダウンロードが実行される場合、例えば、ユーザが屋外において携帯端末を利用している際に、コンテンツ配信サーバに対して、コンテンツの配信を要求すると、ユーザの利用中の携帯端末とサーバ間の認証が実行され、携帯端末が正当である場合にコンテンツが送信される。また、ユーザが屋内においてP Cを利用している際に、コンテンツ配信サーバに対して、コンテンツの配信を要求すると、ユーザの利用中のP Cとサーバ間の認証が実行され、15 P Cが正当である場合にコンテンツが送信され、ダウンロードが可能になる。すなわち、コンテンツ配信サーバは、コンテンツのダウンロード先の機器との認証を行なって、ダウンロードの許可を行なうことになる。

20 ダウンロード対象となるコンテンツは多様化しており、携帯電話等の小メモリに格納可能な小容量の例えばミュージックコンテンツ、ゲームプログラム等がある一方、P C等のハードディスクには格納可能であるが、携帯電話等の小メモリには格納不可能な大容量の例えば映画等の動画像コンテンツ等などもダウンロード対象コンテンツとして流通している。

25 ユーザがフラッシュメモリ等の比較的小容量のメモリを有する携帯端末を利用しているときに、大容量の映画等のコンテンツのダウンロードをコンテンツ配信サーバに要求しても、携帯端末のメモリには格納不可能であり、ダウンロード処理をあきらめざる得ないのが現状である。

発明の開示

本発明は、上述の問題点に鑑みてなされたものであり、P C、携帯端末等、複

数のデータ受信可能な情報処理装置を有するユーザが、いずれか1つの機器、例えば携帯端末からコンテンツ配信サーバにアクセスし、ユーザの所有する他の機器、例えばP Cに対するコンテンツ配信サーバからのコンテンツ送信、およびダウンロード処理をセキュアに実行可能としたコンテンツ配信システム、コンテンツ配信方法、および情報処理装置、並びにコンピュータ・プログラムを提供することを目的とする。

本発明の第1の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する第1の情報処理装置と、

10 コンテンツのダウンロード先として指定される第2の情報処理装置と、

前記第1の情報処理装置からのコンテンツダウンロード要求を受信して、前記第2の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有し、

前記第1の情報処理装置は、

15 前記第2の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信サーバに送信する処理を実行し、

前記コンテンツ配信サーバは、

前記チケットの電子署名の検証を実行し、該検証に成功したことを条件として、前記第2の情報処理装置が前記第1の情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第2の情報処理装置に対するコンテンツ送信を実行する構成を有することを特徴とするコンテンツ配信システムにある。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第1の情報処理装置と、前記第2の情報処理装置は、共有する秘密鍵としてのホームネットエリア共有秘密鍵 [K s e c] を有し、前記第1の情報処理装置は、前記ホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K s e c, K s i g)] を、コンテンツ配信サーバを介して第2の情報処理装置に送信する処理を実行し、前記第2の情報処理装置は、前記ホームネットエリア共有秘密鍵 [K s e c] による暗号化鍵データ [E (K s e c, K s i g)]

の復号により取得したコンテンツ署名用鍵 [K s i g] を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第 1 の
5 情報処理装置と、前記第 2 の情報処理装置は、共有する秘密鍵としてのホームネットエリア共有秘密鍵 [K s e c] を有し、前記第 1 の情報処理装置は、前記ホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E (K s e c, H (M))] を、コンテンツ配信サーバを介して第 2 の情報
10 処理装置に送信する処理を実行し、前記第 2 の情報処理装置は、前記ホームネットエリア共有秘密鍵 [K s e c] による暗号化ハッシュ値 [E (K s e c, H (M))] の復号により取得したコンテンツのハッシュ値 [H (M)] を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第 1 の
15 情報処理装置と、前記第 2 の情報処理装置は、それぞれ公開鍵暗号方式の公開鍵、秘密鍵を有し、前記第 1 の情報処理装置は、該第 1 の情報処理装置の秘密鍵 [K __ S E C __ M B L] を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K __ S E C __ M B L, K s i g)] を、コンテンツ配信サーバを介して第 2 の情報処理装置に送信する
20 処理を実行し、前記第 2 の情報処理装置は、前記第 1 の情報処理装置の公開鍵 [K __ P U B __ M B L] による暗号化鍵データ [E (K __ S E C __ M B L, K s i g)] の復号により取得したコンテンツ署名用鍵 [K s i g] を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行する構成であることを特徴とする。
25

さらに、本発明のコンテンツ配信システムの一実施態様において、前記第 1 の情報処理装置と、前記第 2 の情報処理装置は、それぞれ公開鍵暗号方式の公開鍵、秘密鍵を有し、前記第 1 の情報処理装置は、該第 1 の情報処理装置の秘密鍵 [K __ S E C __ M B L] を適用して、前記コンテンツ配信サーバの生成したコンテン

ツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E (K__S E C__M B L, H (M))] を、コンテンツ配信サーバを介して第 2 の情報処理装置に送信する処理を実行し、前記第 2 の情報処理装置は、前記第 1 の情報処理装置の公開鍵 [K__P U B__M B L] による暗号化ハッシュ値 [E (K__S E C__M B L, H (M))] の復号により取得したコンテンツのハッシュ値 [H (M)] を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記チケットは、前記第 1 の情報処理装置と、前記第 2 の情報処理装置各々の識別子 (I D) を含むデータに対して、前記第 2 の情報処理装置の秘密鍵による電子署名がなされたチケットであり、前記コンテンツ配信サーバは、前記第 2 の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証を実行する構成であることを特徴とする。

さらに、本発明のコンテンツ配信システムの一実施態様において、前記コンテンツ配信サーバは、前記チケットの電子署名の検証処理として、以下の処理 (a) 前記第 2 の情報処理装置の公開鍵証明書の署名 (認証局署名) 検証による公開鍵証明書の正当性確認処理、(b) 正当性の確認された公開鍵証明書からの前記第 2 の情報処理装置の公開鍵の取得処理、(c) 取得した前記第 2 の情報処理装置の公開鍵を適用した前記第 2 の情報処理装置のチケットの署名検証処理、の各処理を実行する構成であることを特徴とする。

さらに、本発明の第 2 の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する第 1 の情報処理装置と、コンテンツのダウンロード先として指定される第 2 の情報処理装置と、前記第 1 の情報処理装置からのコンテンツダウンロード要求を受信して、前記第 2 の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有するコンテンツ配信システムにおけるコンテンツ配信方法であり、

前記第 1 の情報処理装置において、

前記第 2 の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信

サーバに送信するステップと、

前記コンテンツ配信サーバにおいて、

前記チケットの電子署名の検証を実行するステップと、

前記検証に成功したことを条件として、前記第2の情報処理装置が前記第1の
5 情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第2
の情報処理装置に対するコンテンツ送信を実行するステップと、
を有することを特徴とするコンテンツ配信方法にある。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ
配信方法において、前記第1の情報処理装置は、前記第1の情報処理装置と、前
10 記第2の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵
[K s e c]を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名
用鍵[K s i g]を暗号化した暗号化鍵データ[E (K s e c, K s i g)]を、
コンテンツ配信サーバを介して第2の情報処理装置に送信する処理を実行し、前
記第2の情報処理装置は、前記ホームネットエリア共有秘密鍵[K s e c]によ
15 る暗号化鍵データ[E (K s e c, K s i g)]の復号により取得したコンテン
ツ署名用鍵[K s i g]を適用して、コンテンツ配信サーバからの受信コンテン
ツの署名検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ
配信方法において、前記第1の情報処理装置は、前記第1の情報処理装置と、前
20 記第2の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵
[K s e c]を適用して、前記コンテンツ配信サーバの生成したコンテンツのハ
ッシュ値[H (M)]を暗号化した暗号化ハッシュ値[E (K s e c, H (M))]を、
コンテンツ配信サーバを介して第2の情報処理装置に送信する処理を実行し、
前記第2の情報処理装置は、前記ホームネットエリア共有秘密鍵[K s e c]に
25 よる暗号化ハッシュ値[E (K s e c, H (M))]の復号により取得したコン
テンツのハッシュ値[H (M)]を適用して、コンテンツ配信サーバからの受信
コンテンツの検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ
配信方法において、前記第1の情報処理装置は、該第1の情報処理装置の秘密鍵

[K__SEC__MBL] を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K__SEC__MBL, K s i g)] を、コンテンツ配信サーバを介して第 2 の情報処理装置に送信する処理を実行し、前記第 2 の情報処理装置は、前記第 1 の情報処理装置の公開鍵 [K__PUB__MBL] による暗号化鍵データ [E (K__SEC__MBL, K s i g)] の復号により取得したコンテンツ署名用鍵 [K s i g] を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ配信方法において、前記第 1 の情報処理装置は、該第 1 の情報処理装置の秘密鍵 [K__SEC__MBL] を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E (K__SEC__MBL, H (M))] を、コンテンツ配信サーバを介して第 2 の情報処理装置に送信する処理を実行し、前記第 2 の情報処理装置は、前記第 1 の情報処理装置の公開鍵 [K__PUB__MBL] による暗号化ハッシュ値 [E (K__SEC__MBL, H (M))] の復号により取得したコンテンツのハッシュ値 [H (M)] を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記チケットは、前記第 1 の情報処理装置と、前記第 2 の情報処理装置各々の識別子 (ID) を含むデータに対して、前記第 2 の情報処理装置の秘密鍵による電子署名がなされたチケットであり、前記コンテンツ配信サーバは、前記第 2 の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証を実行することを特徴とする。

さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ配信サーバは、前記チケットの電子署名の検証処理として、(a) 前記第 2 の情報処理装置の公開鍵証明書署名 (認証局署名) 検証による公開鍵証明書の正当性確認処理、(b) 正当性の確認された公開鍵証明書からの前記第 2 の情報処理装置の公開鍵の取得処理、(c) 取得した前記第 2 の情報処理装置の公開鍵を適用した前記第 2 の情報処理装置のチケットの署名検証処理、の各処理を実行する

ことを特徴とする。

さらに、本発明の第3の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する情報処理装置であり、

- 5 コンテンツのダウンロード先の第2の情報処理装置の電子署名がなされたチケットを格納した記憶手段と、

前記記憶手段に格納した前記チケットを含むコンテンツダウンロード要求コマンドを生成する制御手段と、

- 10 前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サーバに対して送信する通信手段と、

を有することを特徴とする情報処理装置にある。

- さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制御手段は、該情報処理装置と、前記第2の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信
- 15 サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K s e c, K s i g)] を、前記第2の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。

- さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制御手段は、該情報処理装置と、前記第2の情報処理装置の共有する秘密鍵としての
- 20 ホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E (K s e c, H (M))] を、前記第2の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。

- さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制御手段は、該情報処理装置の秘密鍵 [K __ S E C __ M B L] を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K __ S E C __ M B L, K s i g)] を、前記第2の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。
- 25

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置の制

御手段は、該情報処理装置の秘密鍵 [K__SEC__MBL] を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E (K__SEC__MBL, H (M))] を、前記第 2 の情報処理装置に対する送信データとして生成する構成を有することを特徴とする。

5 さらに、本発明の第 4 の側面は、

自装置と異なるダウンロード先を指定したコンテンツダウンロード要求処理を実行するコンピュータ・プログラムであり、

コンテンツのダウンロード先の第 2 の情報処理装置の電子署名がなされたチケットを取得するステップと、

10 前記チケットを含むコンテンツダウンロード要求コマンドを生成するステップと、

前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サーバに対して送信するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

15 さらに、本発明の第 5 の側面は、

コンテンツの送信処理を実行するコンピュータ・プログラムであり、

第 1 の情報処理装置から自装置と異なるダウンロード先として第 2 の情報処理装置を指定したコンテンツダウンロード要求処理を受信するステップと、

20 前記コンテンツダウンロード要求に含まれるダウンロード先の第 2 の情報処理装置の電子署名がなされたチケットに含まれる電子署名検証処理を実行するステップと、

前記検証に成功したことを条件として、前記第 2 の情報処理装置に対するコンテンツ送信を実行するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

25 なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CD や FD、MO などの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供すること

により、コンピュータ・システム上でプログラムに応じた処理が実現される。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

図 1 は、本発明のコンテンツ配信システムの概要を説明する図である。

図 2 は、本発明のコンテンツ配信システムにおけるホームネットエリアのデバイス構成、格納データ等について説明する図である。

図 3 は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例 1 の処理シーケンスを説明する図である。

図 4 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 1 におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図 5 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 1 におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図 6 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 1 におけるダウンロード先の装置であるホーム P C の処理を説明するフローチャートを示す図である。

図 7 は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例 2 の処理シーケンスを説明する図である。

図 8 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 2 におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図 9 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 2 におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図 10 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 2 におけるダウンロード先の装置であるホーム P C の処理を説明するフローチャートを示す図である。

す図である。

図 1 1 は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例 3 の処理シーケンスを説明する図である。

図 1 2 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 3 におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図 1 3 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 3 におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図 1 4 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 3 におけるダウンロード先の装置であるホーム P C の処理を説明するフローチャートを示す図である。

図 1 5 は、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例 4 の処理シーケンスを説明する図である。

図 1 6 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 4 におけるダウンロード要求装置である携帯情報端末の処理を説明するフローチャートを示す図である。

図 1 7 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 4 におけるコンテンツ配信サーバの処理を説明するフローチャートを示す図である。

図 1 8 は、本発明のコンテンツ配信システムのコンテンツ配信処理例 4 におけるダウンロード先の装置であるホーム P C の処理を説明するフローチャートを示す図である。

図 1 9 は、本発明のコンテンツ配信システムにおけるホーム P C、携帯情報端末等の情報処理装置の構成例を示す図である。

図 2 0 は、本発明のコンテンツ配信システムにおけるコンテンツ配信サーバの構成例を示す図である。

発明を実施するための最良の形態

[システム概要]

図 1 に本発明のコンテンツ配信システムが適用可能なコンテンツ配信構成例を

示す。コンテンツの配信は、コンテンツ配信サーバ150が様々なユーザ機器に対して実行する。図1には、ユーザサイト110にユーザの所有する複数の情報端末を示している。ホームPC120は、例えばハードディスク等の大容量の記憶媒体（ホームストレージ（HS））を有し、ユーザの自宅に備えられた情報処理装置である。また、ユーザサイト110には、携帯電話、PDA等の携帯情報端末130があり、これらの携帯情報端末130は、例えばユーザの外出時等に携帯可能なモバイル型の情報処理装置である。

ユーザは、ホームストレージを有するホームPC120、携帯情報端末130のそれぞれを用いて、コンテンツ配信サーバ150にアクセスし、各接続機器とコンテンツ配信サーバ150間において認証処理、例えば公開鍵暗号方式、または共通鍵暗号方式等に従った認証を実行し、機器の正当性、すなわち、コンテンツ配信サーバがコンテンツの利用を認めた機器であるかを確認して、確認の後、コンテンツの送信、ダウンロード処理を実行する。これらの処理は、ダウンロード対象となる機器との直接認証であり、従来と同様の処理である。

さらに、本発明のシステムでは、例えば携帯情報端末130からコンテンツ配信サーバ150にアクセスを実行し、コンテンツ送信、ダウンロード処理先として、携帯情報端末130ではなく、ホームPC120を指定して、コンテンツ配信サーバ150からホームPC120に対するコンテンツ送信、ホームPC120におけるダウンロードを実行可能とする。

例えば、外出先で携帯電話を利用するユーザが、携帯電話を利用してコンテンツ配信サーバにアクセスして、映画等の動画データのような大容量コンテンツのダウンロード先としてホームPCを指定して、コンテンツ配信サーバからホームPCに対する動画コンテンツの送信、ダウンロード処理を実行させる。

従来、コンテンツ配信サーバ150は、ダウンロード対象機器に対する認証の成立を条件としてコンテンツを送信ダウンロード処理の実行を可能としていた。本発明のシステムでは、携帯情報端末130を利用するユーザが携帯情報端末130を利用してコンテンツ配信サーバ150にアクセスし、ホームPC120に変わってホームPCが信用できるユーザ機器であり、正当なコンテンツ利用権を持つ機器であることの証明処理としての代理認証を実行する。コンテンツ配信サ

ーバ150は、この代理認証の成立を条件として、ホームPC120に対するコンテンツ送信を実行する。

図1に示す、ホームPC120と、携帯情報端末130のように、コンテンツ配信サーバに対するアクセス機器、および該アクセス機器からコンテンツのダウンロード先として指定可能な機器、これらの複数のユーザ機器は、予め、相互に
5 デバイス証明書となるデバイスチケットを交換し、またこれらのユーザ機器における共有秘密鍵としてのホームネットエリア共有秘密鍵を各機器の記憶手段に格納する。

図2にユーザ機器の格納情報、およびユーザ機器間で実行される処理を説明する図を示す。なお、以下の説明におけるデータ、あるいは式等の表示として、携帯情報端末をMBL (Mobile)、ホームPCをHS (Home Storage) として略記する。
10

携帯情報端末130は、製造時に各機器にユニークな識別子としての機器ID [ID__MBL] が割り当てられ、各機器のメモリに格納される。この機器ID
15 は書き換え不可能な固定IDである。また、通信のためのアドレス、例えばIPv6に従ったIPアドレス [ADD__MBL] が設定される。

インターネットにおいて、通信プロトコルとしてIP (Internet Protocol) が用いられ、現在多く使用されているIPはIPv4であり、これは発信元／宛先として32ビットからなるアドレス (IPアドレス) である。しかし、IPv4
20 の限られたアドレス空間、すなわちグローバルアドレスの枯渇が問題となっており、これを解決するのが、IPアドレス空間を32ビットから128ビットに拡張したIPv6 (Internet Protocol version 6) である。IPv6アドレスは、上位64ビットの経路情報 (ネットワークプレフィックス: Network Prefix) [ADD__NET__A] と、下位64ビットの、個々の通信端末、すなわちホストを
25 識別するホストアドレスとから構成される。上述の機器ID [ID__MBL] をIPv6アドレスの下位ビットのホストアドレスとして利用し、IPアドレス [ADD__MBL] を [ADD__NET__A | ID__MBL] として設定することができる。

さらに、携帯情報端末130は、コンテンツ配信に係る決済処理の際の認証を

行なう決済サービス用認証サーバ（CR）から発行されるユーザ証明書 [Cert_User] を有する。ユーザ証明書は、コンテンツ配信サーバからのコンテンツダウンロードサービスを行なおうとするユーザが、決済処理に必要な情報を決済サービス用認証サーバ（CR）に届け出ることにより、決済サービス用認証サーバ（CR）が発行する証明書である。

ユーザ証明書 [Cert_User] は、ユーザID [ID_USR] と、ユーザの公開鍵 [K_PUB_USR] とをメッセージとして、決済サービス用認証サーバ（CR）の秘密鍵 [K_SEC_CR] で電子署名をしたデータ、すなわち、[Cert_User] = [Sig (K_SEC_CR, (ID_USR, K_PUB_USR))] である。なお、電子署名は、例えば、一方向性関数としてのハッシュ関数を適用し、所定の鍵に基づいてハッシュ関数を実行することによって生成されるハッシュ値が用いられる。なお、Sig (A, B) は、Aを適用したBに対する電子署名データを意味するものとする。

電子署名の付与されたデータを受信した受信者は、自己の所有する鍵に基づいて同様にハッシュ値を算出し、データに付与されているハッシュ値との一致を判定することでデータの改竄のないことを確認することができる。

携帯情報端末 130 は、決済サービス用認証サーバ（CR）から発行されるユーザ証明書 [Cert_User] を自己の所有する秘密鍵 [K_SEC_MBL] で署名して、[Sig (K_SEC_MBL, Cert_User)] としてメモリに保存する。

一方、ホームPC 120 は、製造時に各機器にユニークな識別子としての機器ID [ID_HS] が割り当てられ、メモリに格納される。この機器IDは書き換え不可能な固定IDである。また、通信のためのアドレス、例えばIPv6に従ったIPアドレス [ADD_HS] が設定される。このアドレスは、上述の携帯情報端末のアドレスと同様、IPv6アドレスの上位64ビットの経路情報（ネットワークプレフィックス：Network Prefix）[ADD_NET_B] に、下位64ビットとしての上述の機器ID [ID_HS] を利用し、[ADD_HS] を [ADD_NET_B | ID_HS] として設定することができる。

さらに、ホームPC 120 は、携帯情報端末 130 と同様、コンテンツ配信に

係る決済処理の際の認証を行なう決済サービス用認証サーバ（CR）から発行されるユーザ証明書 [Cert_User] を格納する。ホームPC120は、この決済サービス用認証サーバ（CR）から発行されるユーザ証明書 [Cert_User] を自己の所有する秘密鍵 [K_SEC_HS] で署名して、[Sig (K_SEC_HS, Cert_User)] としてメモリに保存する。

さらに、ホームPC120は、ホームネットエリア共有秘密鍵 [Ksec] を有する。このホームネットエリア共有秘密鍵 [Ksec] は、上述したコンテンツ配信サーバとの代理認証を実行するアクセス機器（ここでは携帯情報端末130）に対して必要に応じて送信され、アクセス機器にも格納される。

10 携帯情報端末130、ホームPC120は、それぞれ上述したデータをそれぞれの記憶手段としてのメモリに格納しているが、上述したコンテンツ配信サーバからの他機器に対するダウンロードサービスを実行するために、図2に示すデータ201をホームPC120から携帯情報端末130に送信し、データ202を携帯情報端末130からホームPC120に対して送信する。

15 このデータの送受信は、2者間で同じホームネットエリアに属することを個人認証等の手段を通して確認した上で行われ、他の個所にチケットが流出してはならない。交換されたチケットは、公開鍵ペアの秘密鍵を用いて受け取り手の署名を付加することにより、安全に保持される。

ホームPC120から携帯情報端末130に送信されるデータ201は、ホームPCチケット [Ticket_HS]、およびホームネットエリア共有秘密鍵 [Ksec] である。また、携帯情報端末130からホームPC120に対して送信されるデータ202は、携帯情報端末チケット [Ticket_MBL] である。

25 機器Aから機器Bに対して発行されるチケットは、機器AのID [ID_A] と、機器BのID [ID_B] と、機器Aの公開鍵 [K_PUB_A] をメッセージとして、該メッセージに機器Aの秘密鍵 [K_SEC_A] で電子署名をしたデータ、すなわち、[Sig (K_SEC_A, (ID_A, ID_B, K_PUB_A))] である。

すなわち、ホームPC120から携帯情報端末130に送信されるデータ20

1としてのホームPCチケット[Ticket_HS]は、ホームPC120のID[ID_HS]と、携帯情報端末130のID[ID_MBL]と、ホームPC120の公開鍵[K_PUB_HS]をメッセージとして、該メッセージにホームPC120の秘密鍵[K_SEC_HS]で電子署名をしたデータ、すな
5 わち、[Sig(K_SEC_HS, (ID_HS, ID_MBL, K_PUB_HS))]である。ホームPC120から携帯情報端末130には、このホームPCチケット[Ticket_HS]と、さらにホームネットエリア共有秘密鍵[Ksec]が送信される。

なお、後段で説明するコンテンツ配信処理例3、4では、公開鍵、秘密鍵ペア
10 をKsecの代わりに利用する方式であり、通常の公開鍵の利用法と異なる方式を採用している。すなわち、例えばKsecの代わりに利用される公開鍵ペアは専用に別に用意され、ホームエリア内にのみ公開鍵が公開される。これにより、Ksigを取得できるのは、ホームエリア内の機器のみとなる。本方式は、Ksecを共有する構成と異なり、機器毎に個別の秘密鍵を持つので、個別の機器を
15 セキュリティ的に区別した利用形態に適している。

一方、携帯情報端末130からホームPC120に送信されるデータ202としての携帯情報端末チケット[Ticket_MBL]は、携帯情報端末130のID[ID_MBL]と、ホームPC120のID[ID_HS]と、携帯情報端末130の公開鍵[K_PUB_MBL]をメッセージとして、該メッセー
20 ジに携帯情報端末130の秘密鍵[K_SEC_MBL]で電子署名をしたデータ、すなわち、[Sig(K_SEC_MBL, (ID_MBL, ID_HS, K_PUB_MBL))]である。

携帯情報端末130は、ホームPC120から送信されるホームPCチケット[Ticket_HS]と、ホームネットエリア共有秘密鍵[Ksec]をメモ
25 りに格納し、一方、ホームPC120は、携帯情報端末130から送信される携帯情報端末チケット[Ticket_MBL]をメモリに格納する。

図2の構成において、携帯情報端末130は、自装置と異なるダウンロード先としてホームPC120を指定したコンテンツダウンロード要求を実行する情報処理装置であり、コンテンツのダウンロード先としての情報処理装置（ホームP

C 1 2 0) の電子署名がなされたチケットを記憶手段としてのメモリに格納し、
携帯情報端末 1 3 0 の C P U 等の制御手段において、メモリに格納したチケット
を含むコンテンツダウンロード要求コマンドを生成し、生成したコンテンツダウ
ンロード要求コマンドを通信手段を介してコンテンツ配信サーバに対して送信す
5 る。以下、本発明のシステムにおけるコンテンツ配信処理の詳細について説明す
る。

[コンテンツ配信処理例 1]

以下、本発明のコンテンツ配信システムにおけるコンテンツ配信処理例につい
10 て、複数の処理態様を順次、説明する。なお、以下の説明では、携帯情報端末が
コンテンツ配信サーバにアクセスを実行して、ホームストレージを備えたホーム
P C に対するコンテンツダウンロードを実行する処理として説明するが、この逆
の処理、すなわち、ホーム P C からコンテンツ配信サーバにアクセスを実行し、
携帯情報端末に対してコンテンツのダウンロードを実行することも同様の処理過
15 程を実行することで可能であり、ユーザ所有の端末のコンテンツ配信サーバに対
するアクセス処理端末、ダウンロード処理端末は任意の組み合わせが可能である。

まず、図 3 乃至図 6 を参照して、コンテンツ配信処理例 1 について説明する。
図 3 は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行
する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロ
ードする大容量記憶媒体としてのホームストレージを備えたホーム P C との 3 者
20 間で実行する処理を示すシーケンス図である。図 4 は携帯情報端末の処理を示す
フローチャート、図 5 はコンテンツ配信サーバの処理を示すフローチャート、図
6 はホーム P C の処理を示すフローチャートである。

図 3 を参照して、本実施例の処理について説明する。図 3 において処理は、図
25 に示す番号 (1) ~ (9) の順に進行する。

また、図 3 において、携帯情報端末 1 3 0 の識別子 (I D) は [I D _ M B L] 、
アドレスは [A D D _ M B L] であり、これは、 [A D D _ N E T _ A | I D _
M B L] に相当する。また、携帯情報端末 1 3 0 は、ホームネットエリア共有秘
密鍵 [K s e c] を有する。また、ホーム P C 1 2 0 の識別子 (I D) は [I D

__HS]、アドレスは[ADD__HS]であり、これは、[ADD__NET__B
|ID__HS]に相当する。また、ホームPC120は、ホームネットエリア共
有秘密鍵[Ksec]を有する。また、コンテンツ配信サーバ150の識別子(ID)
5 DD__NET__X|ID__SRV]に相当するものとする。

まず、(1)の処理として、携帯情報端末130は、コンテンツ配信サーバ1
50に対して、コンテンツのダウンロードを要求する。このダウンロード要求に
は、ダウンロード先となる機器、ここではホームPC120から受領したホーム
PCチケット[Ticket__HS]、および、ダウンロード先となるホームP
10 C120の公開鍵を格納した公開鍵証明書[K__PUB__HS-cert]が含ま
れる。なお、公開鍵証明書は、別途認証局(CA)から取得する構成としても
よい。ホームPCチケット[Ticket__HS]は、ホームPC120のID
[ID__HS]と、携帯情報端末130のID[ID__MBL]と、ホームPC
120の公開鍵[K__PUB__HS]をメッセージとして、該メッセージにホー
15 ムPC120の秘密鍵[K__SEC__HS]で電子署名をしたデータ、すなわち、
[Sig(K__SEC__HS,(ID__HS,ID__MBL,K__PUB__HS))]
である。

携帯情報端末130からホームPCチケット[Sig(K__SEC__MBL,
(Ticket__HS))]、ホームPC120の公開鍵証明書[K__PUB__
20 HS-cert]を受信したコンテンツ配信サーバ150は、携帯情報端末13
0の公開鍵証明書から取得される携帯情報端末130の公開鍵を用いて、ホーム
PCチケット[Sig(K__SEC__MBL,(Ticket__HS))]の署
名検証を実行し、(2)の処理としてホームPCチケット[Ticket__HS]
の検証処理を実行する。この検証処理の手順は、(a)ホームPC120の公開
25 鍵証明書[K__PUB__HS-cert]の署名(認証局署名)検証による公開
鍵証明書[K__PUB__HS-cert]の正当性確認処理、(b)正当性の確
認された公開鍵証明書[K__PUB__HS-cert]からのホームPC120
の公開鍵[K__PUB__HS]の取得処理、(c)取得したホームPC120の
公開鍵[K__PUB__HS]を適用したホームPCチケット[Ticket__H

S]、すなわち、 $[Sig(K_SEC_HS, (ID_HS, ID_MBL, K_PUB_HS))]$ の署名検証処理である。

この手続き、すなわちホームPCチケット[Ticket_HS]の検証により、ホームPCチケット[Ticket_HS]が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ150は、(3)の処理として、コンテンツ署名用鍵[Ksig]を生成する。これは例えば乱数発生器により生成される乱数に基づいて生成する一時的に使用するための鍵である。次に、(4)の処理として、コンテンツ配信サーバ150は、生成したコンテンツ署名用鍵[Ksig]を携帯情報端末130に送信する。

10 コンテンツ署名用鍵[Ksig]を受信した携帯情報端末130は、(5)の処理として、ホームネットエリア共有秘密鍵[Ksec]を適用してコンテンツ署名用鍵[Ksig]を暗号化して、暗号化鍵データ[E(Ksec, Ksig)]を生成する。この暗号化処理には、例えばDES暗号化処理が適用される。なお、E(A, B)は、BをAによって暗号化したデータを示すものとする。次に、携帯情報端末130は、(6)の処理として、生成した暗号化鍵データ[E(Ksec, Ksig)]をコンテンツ配信サーバ150に送信する。

20 (7)の処理として、コンテンツ配信サーバ150は、先に生成したコンテンツ署名用鍵[Ksig]を適用して、ダウンロード対象のコンテンツ(M)に対する電子署名を行ない、署名されたコンテンツデータとしての[Sig(Ksig, M)]を生成する。

次に(8)の処理として、コンテンツ配信サーバ150は、ダウンロード先となるホームPC120に対して、署名されたコンテンツデータとしての[Sig(Ksig, M)]と、先の(5)の処理において、携帯情報端末130から受信した暗号化鍵データ[E(Ksec, Ksig)]を送信する。

25 次に、署名されたコンテンツデータとしての[Sig(Ksig, M)]と、暗号化鍵データ[E(Ksec, Ksig)]を受信したホームPC120は、(9)の処理として、自己の所有するホームネットエリア共有秘密鍵[Ksec]を適用して、受信した暗号化鍵データ[E(Ksec, Ksig)]の復号処理を実行して、コンテンツ署名用鍵[Ksig]を取り出して、署名されたコンテ

ンツデータとしての [S i g (K s i g , M)] の署名検証処理を実行する。この署名検証処理において、コンテンツ (M) のデータ改竄のないことが立証されたことを条件としてコンテンツの格納または再生処理を実行する。

次に、図 4 乃至図 6 のフローチャートを参照して、携帯情報端末 1 3 0 の処理、
5 コンテンツ配信サーバ 1 5 0 の処理、およびホーム P C 1 2 0 の処理のそれぞれについて説明する。

まず、図 4 のフローチャートを参照して携帯情報端末 1 3 0 の処理手順について説明する。ステップ S 1 1 1 において、携帯情報端末 1 3 0 は、ダウンロード先となる機器のデバイスチケット、ここではホーム P C 1 2 0 のホーム P C チケット [T i c k e t _ H S] を含むデータをコンテンツ配信サーバ 1 5 0 に送信
10 して、コンテンツのダウンロードを要求する。

ステップ S 1 1 2 において、携帯情報端末 1 3 0 は、コンテンツ配信サーバ 1 5 0 の生成したコンテンツ署名用鍵 [K s i g] を受信する。

ステップ S 1 1 3 において、コンテンツ署名用鍵 [K s i g] を受信した携帯
15 情報端末 1 3 0 は、ホームネットエリア共有秘密鍵 [K s e c] を適用してコンテンツ署名用鍵 [K s i g] を暗号化して、暗号化鍵データ [E (K s e c , K s i g)] を生成し、ステップ S 1 1 4 において、生成した暗号化鍵データ [E (K s e c , K s i g)] をコンテンツ配信サーバ 1 5 0 に送信する。

以上の処理が、携帯情報端末 1 3 0 とコンテンツ配信サーバ 1 5 0 間で実行さ
20 れるコンテンツダウンロード要求処理における携帯情報端末 1 3 0 側の処理である。

次に、図 5 を参照して、携帯情報端末 1 3 0 からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ 1 5 0 の処理について説明する。

まず、コンテンツ配信サーバ 1 5 0 は、ステップ S 1 2 1 において、携帯情報
25 端末 1 3 0 から、ダウンロード先のデバイスチケット、ここではホーム P C 1 2 0 のホーム P C チケット [T i c k e t _ H S] を含むデータをダウンロードコマンドとして受信する。

携帯情報端末 1 3 0 からホーム P C チケット [T i c k e t _ H S] を含むダウンロードコマンドを受信したコンテンツ配信サーバ 1 5 0 は、ステップ S 1 2

2において、ホームPCチケット[Ticket__HS]の検証処理を実行する。
この検証処理は、先に説明したように、ホームPC120の公開鍵証明書[K__PUB__HS-cert]の署名(認証局署名)検証による公開鍵証明書[K__PUB__HS-cert]の正当性確認処理、正当性の確認された公開鍵証明書
5 [K__PUB__HS-cert]からのホームPC120の公開鍵[K__PUB__HS]の取得処理、得したホームPC120の公開鍵[K__PUB__HS]を適用したホームPCチケット[Ticket__HS]、すなわち、[Sig(K__SEC__HS, (ID__HS, ID__MBL, K__PUB__HS))]の署名検証処理を順次行なうことによって実行される。

10 ステップS123において、チケット検証が不成立と判定された場合は、チケット、すなわちホームPCチケット[Ticket__HS]が偽造されたものである可能性があり、ステップS129に進み、エラーメッセージを携帯情報端末130に送信して処理を終了する。この場合は、コンテンツのダウンロード処理は実行されない、

15 ステップS123において、チケット検証が成立したと判定された場合は、ステップS124に進み、コンテンツ署名用鍵[Ksig]を生成し、ステップS125において、生成したコンテンツ署名用鍵[Ksig]を携帯情報端末130に送信する。

次に、コンテンツ配信サーバ150は、ステップS126において、ホームネットエリア共有秘密鍵[Ksec]を適用してコンテンツ署名用鍵[Ksig]を暗号化した暗号化鍵データ[E(Ksec, Ksig)]を携帯情報端末130から受信する。

次に、コンテンツ配信サーバ150は、ステップS127において、先に生成したコンテンツ署名用鍵[Ksig]を適用して、ダウンロード対象のコンテンツ(M)に対する電子署名を行ない、署名されたコンテンツデータとしての[Sig(Ksig, M)]を生成する。
25

次に、コンテンツ配信サーバ150は、ステップS128において、ダウンロード先となるホームPC120に対して、署名されたコンテンツデータとしての[Sig(Ksig, M)]と、先に携帯情報端末130から受信した暗号化鍵デ

ータ $[E(K_{sec}, K_{sig})]$ を送信する。

以上の処理が、携帯情報端末 130 からコンテンツダウンロード要求を受信した配信サーバ 150 の処理である。

次に、図 6 を参照して、コンテンツ配信サーバ 150 からコンテンツのダウンロードが実行されるホーム PC 120 の処理について説明する。

ホーム PC 120 は、ステップ S 131 において、コンテンツ配信サーバ 150 から、署名されたコンテンツデータとしての $[Sig(K_{sig}, M)]$ と、暗号化鍵データ $[E(K_{sec}, K_{sig})]$ を受信する。

ステップ S 132 において、ホーム PC 120 は、自己の所有するホームネットエリア共有秘密鍵 $[K_{sec}]$ を適用して、受信した暗号化鍵データ $[E(K_{sec}, K_{sig})]$ の復号処理を実行する。

ステップ S 133 において、復号に失敗した場合は、ホームネットエリア共有秘密鍵 $[K_{sec}]$ が携帯情報端末 130 の有する鍵と異なるなど、正当なホームネットエリア共有秘密鍵でない可能性があり、ステップ S 137 に進み、受信コンテンツを破棄する。

ステップ S 133 において、復号に成功した場合は、復号によって取得したコンテンツ署名用鍵 $[K_{sig}]$ を適用して、署名されたコンテンツデータとしての $[Sig(K_{sig}, M)]$ の署名検証処理を実行する。この署名検証に不成功の場合 (S 135 で No) は、コンテンツ改竄の可能性があり、ステップ S 137 に進み、受信コンテンツを破棄する。

署名検証に成功した場合 (S 135 で Yes) は、ステップ S 136 において、受信コンテンツをホーム PC 120 のストレージに格納し、ダウンロード処理を終了する。

以上の処理が、携帯情報端末 130 からコンテンツダウンロード要求を受信した配信サーバ 150 からのコンテンツを受信し、ダウンロードを実行するホーム PC 120 の処理である。

上述したように、本実施例においては、コンテンツ配信サーバ 150 は、携帯情報端末 130 から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末 130 の送付してきたホーム PC チケットに基づ

いて、ホームPC120が、携帯情報端末130の承認しているダウンロード先であることの確認が可能となる。

すなわち、本発明の構成によれば、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームPCが、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

- 10 また、本実施例においては、コンテンツ署名用鍵 [K s i g] を、ホームPC120と携帯情報端末130の共有するホームネットエリア共有秘密鍵 [K s e c] により暗号化して、携帯情報端末130からコンテンツ配信サーバ150を介してダウンロード先であるホームPC120に送信し、ホームPC120において所有するホームネットエリア共有秘密鍵 [K s e c] により復号してコンテンツ署名用鍵 [K s i g] を取得する構成としたので、ホームPC120と携帯情報端末130が同一のホームネットエリア共有秘密鍵 [K s e c] を有することが、ダウンロード先であるホームPC120においてコンテンツ署名用鍵 [K s i g] を取得できる条件となり、同一のホームネットエリア共有秘密鍵 [K s e c] を有する機器間においてのみ、有効なコンテンツのダウンロードが実行可能となる。
- 15 20

[コンテンツ配信処理例2]

- 次に、コンテンツ配信処理例2について説明する。コンテンツ配信処理例2は、コンテンツ配信サーバ150がコンテンツのハッシュ値を算出して、ハッシュ値をホームPC120と携帯情報端末130が有するホームネットエリア共有秘密鍵 [K s e c] で暗号化して、携帯情報端末130からコンテンツ配信サーバ150を介してダウンロード先であるホームPC120に送信する処理を実行する構成例である。
- 25

図7乃至図10を参照して、コンテンツ配信処理例2について説明する。図7

は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロードする大容量記憶媒体としてのホームストレージを備えたホームPCとの3者間で実行する処理を示すシーケンス図である。図8は携帯情報端末の処理を示すフローチャート、図9はコンテンツ配信サーバの処理を示すフローチャート、図10はホームPCの処理を示すフローチャートである。

図7を参照して、本実施例の処理について説明する。図7において処理は、図に示す番号(1)～(9)の順に進行する。

まず、(1)の処理として、携帯情報端末130は、コンテンツ配信サーバ150に対して、コンテンツのダウンロードを要求する。このダウンロード要求には、ダウンロード先となる機器、ここではホームPC120から受領したホームPCチケット[Ticket_HS]、および、ダウンロード先となるホームPC120の公開鍵を格納した公開鍵証明書[K_PUB_HS-cert]が含まれる。ホームPCチケット[Ticket_HS]は、ホームPC120のID[ID_HS]と、携帯情報端末130のID[ID_MBL]と、ホームPC120の公開鍵[K_PUB_HS]をメッセージとして、該メッセージにホームPC120の秘密鍵[K_SEC_HS]で電子署名をしたデータ、すなわち、[Sig(K_SEC_HS, (ID_HS, ID_MBL, K_PUB_HS))]である。

携帯情報端末130からホームPCチケット[Sig(K_SEC_MBL, (Ticket_HS))], ホームPC120の公開鍵証明書[K_PUB_HS-cert]を受信したコンテンツ配信サーバ150は、携帯情報端末130の公開鍵証明書から取得される携帯情報端末130の公開鍵を用いて、ホームPCチケット[Sig(K_SEC_MBL, (Ticket_HS))]の署名検証を実行し、(2)の処理としてホームPCチケット[Ticket_HS]の検証処理を実行する。この検証処理の手順は、(a)ホームPC120の公開鍵証明書[K_PUB_HS-cert]の署名(認証局署名)検証による公開鍵証明書[K_PUB_HS-cert]の正当性確認処理、(b)正当性の確認された公開鍵証明書[K_PUB_HS-cert]からのホームPC120の公開鍵[K_

PUB_HS]の取得処理、(c)取得したホームPC120の公開鍵[K_PUB_HS]を適用したホームPCチケット[Ticket_HS]、すなわち、[Sig(K_SEC_HS, (ID_HS, ID_MBL, K_PUB_HS))]の署名検証処理である。

- 5 この手続き、すなわちホームPCチケット[Ticket_HS]の検証により、ホームPCチケット[Ticket_HS]が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ150は、(3)の処理として、コンテンツのハッシュ値[H(M)]を計算する。次に、(4)の処理として、コンテンツ配信サーバ150は、生成したコンテンツのハッシュ値[H(M)]を携
- 10 帯情報端末130に送信する。

- コンテンツのハッシュ値[H(M)]を受信した携帯情報端末130は、(5)の処理として、ホームネットエリア共有秘密鍵[Ksec]を適用してコンテンツのハッシュ値[H(M)]を暗号化して、暗号化ハッシュ値[E(Ksec, H(M)))]を生成し、(6)の処理として、生成した暗号化ハッシュ値[E(Ksec, H(M)))]をコンテンツ配信サーバ150に送信する。
- 15

- (7)の処理として、コンテンツ配信サーバ150は、暗号化ハッシュ値[E(Ksec, H(M)))]とコンテンツ(M)からなるコンテンツパッケージ[M | E(Ksec, H(M)))]を生成し、(8)の処理として、コンテンツ配信サーバ150は、ダウンロード先となるホームPC120に対して、コンテンツパッケージ[M | E(Ksec, H(M)))]を送信する。
- 20

- 次に、コンテンツパッケージ[M | E(Ksec, H(M)))]を受信したホームPC120は、(9)の処理として、自己の所有するホームネットエリア共有秘密鍵[Ksec]を適用して、受信したコンテンツパッケージ[M | E(Ksec, H(M)))]に含まれる暗号化ハッシュ値[E(Ksec, H(M)))]の復号
- 25 処理を実行して、コンテンツ署名用鍵[Ksig]を取り出して、コンテンツのハッシュ値[H(M)]を取り出し、また、コンテンツ(M)に対するハッシュ値を計算して、両ハッシュ値の一致を確認する。一致している場合は、コンテンツの改竄がないと判定し、不一致の場合は、コンテンツ改竄ありと判定する。検証処理において、コンテンツ(M)のデータ改竄のないことが立証されたことを条

件としてコンテンツの格納または再生処理を実行する。

次に、図8乃至図10のフローチャートを参照して、携帯情報端末130の処理、コンテンツ配信サーバ150の処理、およびホームPC120の処理のそれぞれについて説明する。

5 まず、図8のフローチャートを参照して携帯情報端末130の処理手順について説明する。ステップS211において、携帯情報端末130は、ダウンロード先となる機器のデバイスチケット、ここではホームPC120のホームPCチケット[Ticket_HS]を含むデータをコンテンツ配信サーバ150に送信して、コンテンツのダウンロードを要求する。

10 ステップS212において、携帯情報端末130は、コンテンツ配信サーバ150の生成したコンテンツのハッシュ値[H(M)]を受信する。

15 ステップS213において、コンテンツのハッシュ値[H(M)]を受信した携帯情報端末130は、ホームネットエリア共有秘密鍵[Ksec]を適用してコンテンツのハッシュ値[H(M)]を暗号化して、暗号化ハッシュ値[E(Ksec, H(M))]を生成し、ステップS214において、生成した暗号化ハッシュ値[E(Ksec, H(M))]をコンテンツ配信サーバ150に送信する。

以上の処理が、携帯情報端末130とコンテンツ配信サーバ150間で実行されるコンテンツダウンロード要求処理における携帯情報端末130側の処理である。

20 次に、図9を参照して、携帯情報端末130からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ150の処理について説明する。

25 まず、コンテンツ配信サーバ150は、ステップS221において、携帯情報端末130から、ダウンロード先のデバイスチケット、ここではホームPC120のホームPCチケット[Ticket_HS]を含むデータをダウンロードコマンドとして受信する。

携帯情報端末130からホームPCチケット[Ticket_HS]を含むダウンロードコマンドを受信したコンテンツ配信サーバ150は、ステップS222において、ホームPCチケット[Ticket_HS]の検証処理を実行する。この検証処理は、先に説明したと同様の処理である。

ステップS 2 2 3において、チケット検証が不成立と判定された場合は、チケット、すなわちホームPCチケット[T i c k e t _ H S]が偽造されたものである可能性があり、ステップS 2 2 9に進み、エラーメッセージを携帯情報端末1 3 0に送信して処理を終了する。この場合は、コンテンツのダウンロード処理は実行されない、

ステップS 2 2 3において、チケット検証が成立したと判定された場合は、ステップS 2 2 4に進み、コンテンツのハッシュ値[H (M)]を生成し、ステップS 2 2 5において、生成したコンテンツのハッシュ値[H (M)]を携帯情報端末1 3 0に送信する。

10 次に、コンテンツ配信サーバ1 5 0は、ステップS 2 2 6において、ホームネットエリア共有秘密鍵[K s e c]を適用してコンテンツのハッシュ値[H (M)]を暗号化した暗号化ハッシュ値[E (K s e c , H (M))]を携帯情報端末1 3 0から受信する。

15 次に、コンテンツ配信サーバ1 5 0は、ステップS 2 2 7において、携帯情報端末1 3 0から受信した暗号化ハッシュ値[E (K s e c , H (M))]とコンテンツ(M)からなるコンテンツパッケージ[M | E (K s e c , H (M))]を生成する。

20 次に、コンテンツ配信サーバ1 5 0は、ステップS 2 2 8において、ダウンロード先となるホームPC 1 2 0に対して、コンテンツパッケージ[M | E (K s e c , H (M))]を送信する。

以上の処理が、携帯情報端末1 3 0からコンテンツダウンロード要求を受信した配信サーバ1 5 0の処理である。

次に、図1 0を参照して、コンテンツ配信サーバ1 5 0からコンテンツのダウンロードが実行されるホームPC 1 2 0の処理について説明する。

25 ホームPC 1 2 0は、ステップS 2 3 1において、コンテンツ配信サーバ1 5 0から、コンテンツパッケージ[M | E (K s e c , H (M))]を受信する。

ステップS 2 3 2において、ホームPC 1 2 0は、自己の所有するホームネットエリア共有秘密鍵[K s e c]を適用して、受信したコンテンツパッケージ[M | E (K s e c , H (M))]に含まれる暗号化ハッシュ値[E (K s e c , H (M))]

の復号処理を実行する。

ステップ S 2 3 3 において、復号に失敗した場合は、ホームネットエリア共有秘密鍵 [K s e c] が携帯情報端末 1 3 0 の有する鍵と異なるなど、正当なホームネットエリア共有秘密鍵でない可能性があり、ステップ S 2 3 7 に進み、受信
5 コンテンツを破棄する。

ステップ S 2 3 3 において、復号に成功した場合は、復号によって取得したコンテンツのハッシュ値 [H (M)] と、コンテンツ (M) に基づいて計算により算出したハッシュ値 H (M)' との比較を実行する。この比較において両ハッシュ値が不一致の場合 (S 2 3 5 で N o) は、コンテンツ改竄の可能性があり、ステップ S 2 3 7 に進み、受信コンテンツを破棄する。
10

両ハッシュ値が一致した場合 (S 2 3 5 で Y e s) は、ステップ S 2 3 6 において、受信コンテンツをホーム P C 1 2 0 のストレージに格納し、ダウンロード処理を終了する。

以上の処理が、携帯情報端末 1 3 0 からコンテンツダウンロード要求を受信した配信サーバ 1 5 0 からのコンテンツを受信し、ダウンロードを実行するホーム P C 1 2 0 の処理である。
15

上述したように、本実施例においては、コンテンツ配信サーバ 1 5 0 は、携帯情報端末 1 3 0 から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末 1 3 0 の送付してきたホーム P C チケットに基づいて、ホーム P C 1 2 0 が、携帯情報端末 1 3 0 の承認しているダウンロード先であることの確認が可能となる。すなわち、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホーム P C が、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。
20
25

また、本実施例においては、コンテンツのハッシュ値 [H (M)] を、ホーム P C 1 2 0 と携帯情報端末 1 3 0 の共有するホームネットエリア共有秘密鍵 [K s

ec]により暗号化して、携帯情報端末130からコンテンツ配信サーバ150を介してダウンロード先であるホームPC120に送信し、ホームPC120において所有するホームネットエリア共有秘密鍵[Ksec]により復号してコンテンツのハッシュ値[H(M)]を取得して、コンテンツに基づいてみずから算出するハッシュ値と比較する構成としたので、ホームPC120と携帯情報端末130が同一のホームネットエリア共有秘密鍵[Ksec]を有することが、ダウンロード先であるホームPC120においてハッシュ値の比較できる条件となり、同一のホームネットエリア共有秘密鍵[Ksec]を有する機器間においてのみ、有効なコンテンツのダウンロードが実行可能となる。

10

[コンテンツ配信処理例3]

次に、コンテンツ配信処理例3について説明する。コンテンツ配信処理例3は、コンテンツ配信処理例1, 2で適用したホームネットエリア共有秘密鍵[Ksec]を用いず、一般的な公開鍵方式における公開鍵と秘密鍵の一の鍵を適用した処理を実行する構成例である。コンテンツ配信サーバ150がコンテンツの署名鍵を生成して、署名鍵の暗号化、復号化処理を公開鍵方式によりホームPC120と携帯情報端末130において実行する例である。

図11乃至図14を参照して、コンテンツ配信処理例3について説明する。図11は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロードする大容量記憶媒体としてのホームストレージを備えたホームPCとの3者間で実行する処理を示すシーケンス図である。図12は携帯情報端末の処理を示すフローチャート、図13はコンテンツ配信サーバの処理を示すフローチャート、図14はホームPCの処理を示すフローチャートである。

図11を参照して、本実施例の処理について説明する。図11において処理は、図に示す番号(1)～(9)の順に進行する。ホームPC120と携帯情報端末130のそれぞれは、公開鍵方式の公開鍵、秘密鍵のペアを有する。すなわち、ホームPC120は、[K_PUB_HS], [K_SEC_HS]、携帯情報端末130は、[K_PUB_MBL], [K_SEC_MBL]を有する。さらに、ダ

ダウンロード先の機器であるホームPC120は、ダウンロード要求処理を実行する機器、すなわち携帯情報端末130の公開鍵 [K__PUB__MBL] を取得しているものとする。

まず、(1)の処理として、携帯情報端末130は、コンテンツ配信サーバ150に対して、コンテンツのダウンロードを要求する。このダウンロード要求には、ダウンロード先となる機器、ここではホームPC120から受領したホームPCチケット [Ticket__HS]、および、ダウンロード先となるホームPC120の公開鍵を格納した公開鍵証明書 [K__PUB__HS-cert] が含まれる。ホームPCチケット [Ticket__HS] は、ホームPC120のID [ID__HS] と、携帯情報端末130のID [ID__MBL] と、ホームPC120の公開鍵 [K__PUB__HS] をメッセージとして、該メッセージにホームPC120の秘密鍵 [K__SEC__HS] で電子署名をしたデータ、すなわち、[Sig (K__SEC__HS, (ID__HS, ID__MBL, K__PUB__HS))] である。

携帯情報端末130からホームPCチケット [Sig (K__SEC__MBL, (Ticket__HS))], ホームPC120の公開鍵証明書 [K__PUB__HS-cert] を受信したコンテンツ配信サーバ150は、携帯情報端末130の公開鍵証明書から取得される携帯情報端末130の公開鍵を用いて、ホームPCチケット [Sig (K__SEC__MBL, (Ticket__HS))] の署名検証を実行し、(2)の処理としてホームPCチケット [Ticket__HS] の検証処理を実行する。この検証処理の手順は、上述の処理例1と同様である。ホームPCチケット [Ticket__HS] の検証により、ホームPCチケット [Ticket__HS] が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ150は、(3)の処理として、コンテンツ署名用鍵 [Ksig] を生成する。これは例えば乱数発生器により生成される乱数に基づいて生成する一時的に使用するための鍵である。次に、(4)の処理として、コンテンツ配信サーバ150は、生成したコンテンツ署名用鍵 [Ksig] を携帯情報端末130に送信する。

コンテンツ署名用鍵 [Ksig] を受信した携帯情報端末130は、(5)の処

理として、携帯情報端末 130 の第 2 秘密鍵 [K__SEC2__MBL] を適用してコンテンツ署名用鍵 [Ksig] を暗号化して、暗号化鍵データ [E (K__SEC2__MBL, Ksig)] を生成する。携帯情報端末 130 の第 2 秘密鍵 [K__SEC2__MBL] は、チケットで使用される公開鍵ペアとは別の第 2 の公開鍵ペアを構成する秘密鍵である。この第 2 の公開鍵ペアは、ホームネットエリア内のみで共有される秘密情報である。なお、携帯情報端末 130 の第 2 秘密鍵 [K__SEC2__MBL] を適用したコンテンツ署名用鍵 [Ksig] の暗号化処理は、公開鍵暗号方式による処理であり、秘密鍵で暗号化したデータはペアの公開鍵によって復号可能となる。次に、携帯情報端末 130 は、(6) の処理として、生成した暗号化鍵データ [E (K__SEC2__MBL, Ksig)] をコンテンツ配信サーバ 150 に送信する。

(7) の処理として、コンテンツ配信サーバ 150 は、先に生成したコンテンツ署名用鍵 [Ksig] を適用して、ダウンロード対象のコンテンツ (M) に対する電子署名を行ない、署名されたコンテンツデータとしての [Sig (Ksig, M)] を生成する。

次に (8) の処理として、コンテンツ配信サーバ 150 は、ダウンロード先となるホーム PC 120 に対して、署名されたコンテンツデータとしての [Sig (Ksig, M)] と、先の (5) の処理において、携帯情報端末 130 から受信した暗号化鍵データ [E (K__SEC2__MBL, Ksig)] を送信する。

次に、署名されたコンテンツデータとしての [Sig (Ksig, M)] と、暗号化鍵データ [E (K__SEC2__MBL, Ksig)] を受信したホーム PC 120 は、(9) の処理として、自己の所有する携帯情報端末 130 の公開鍵 [K__PUB2__MBL] を適用して、受信した暗号化鍵データ [E (K__SEC2__MBL, Ksig)] の復号処理を実行して、コンテンツ署名用鍵 [Ksig] を取り出して、署名されたコンテンツデータとしての [Sig (Ksig, M)] の署名検証処理を実行する。この署名検証処理において、コンテンツ (M) のデータ改竄のないことが立証されたことを条件としてコンテンツの格納または再生処理を実行する。

次に、図 12 乃至図 14 のフローチャートを参照して、携帯情報端末 130 の

処理、コンテンツ配信サーバ 150 の処理、およびホーム P C 120 の処理のそれぞれについて説明する。

まず、図 12 のフローチャートを参照して携帯情報端末 130 の処理手順について説明する。ステップ S 311 において、携帯情報端末 130 は、ダウンロード先となる機器のデバイスチケット、ここではホーム P C 120 のホーム P C チケット [T i c k e t _H S] を含むデータをコンテンツ配信サーバ 150 に送信して、コンテンツのダウンロードを要求する。

ステップ S 312 において、携帯情報端末 130 は、コンテンツ配信サーバ 150 の生成したコンテンツ署名用鍵 [K s i g] を受信する。

10 ステップ S 313 において、コンテンツ署名用鍵 [K s i g] を受信した携帯情報端末 130 は、携帯情報端末 130 の秘密鍵 [K _S E C 2 _M B L] を適用してコンテンツ署名用鍵 [K s i g] を暗号化して、暗号化鍵データ [E (K _S E C 2 _M B L, K s i g)] を生成し、ステップ S 314 において、生成した暗号化鍵データ [E (K _S E C 2 _M B L, K s i g)] をコンテンツ配信サーバ 150 に送信する。

以上の処理が、携帯情報端末 130 とコンテンツ配信サーバ 150 間で実行されるコンテンツダウンロード要求処理における携帯情報端末 130 側の処理である。

次に、図 13 を参照して、携帯情報端末 130 からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ 150 の処理について説明する。

まず、コンテンツ配信サーバ 150 は、ステップ S 321 において、携帯情報端末 130 から、ダウンロード先のデバイスチケット、ここではホーム P C 120 のホーム P C チケット [T i c k e t _H S] を含むデータをダウンロードコマンドとして受信する。

25 携帯情報端末 130 からホーム P C チケット [T i c k e t _H S] を含むダウンロードコマンドを受信したコンテンツ配信サーバ 150 は、ステップ S 322 において、ホーム P C チケット [T i c k e t _H S] の検証処理を実行する。この検証処理は、先に説明したように、ホーム P C 120 の公開鍵証明書 [K _P U B _H S - c e r t] の署名（認証局署名）検証による公開鍵証明書 [K _

PUB__HS-cert] の正当性確認処理、正当性の確認された公開鍵証明書
[K__PUB__HS-cert] からのホームPC120の公開鍵 [K__PUB__HS] の取得処理、得たホームPC120の公開鍵 [K__PUB__HS] を
適用したホームPCチケット [Ticket__HS]、すなわち、[Sig (K__
5 SEC__HS, (ID__HS, ID__MBL, K__PUB__HS))] の署名検証処
理を順次行なうことによって実行される。

ステップS323において、チケット検証が不成立と判定された場合は、チケ
ット、すなわちホームPCチケット [Ticket__HS] が偽造されたもので
ある可能性があり、ステップS129に進み、エラーメッセージを携帯情報端末
10 130に送信して処理を終了する。この場合は、コンテンツのダウンロード処理
は実行されない、

ステップS323において、チケット検証が成立したと判定された場合は、ス
テップS324に進み、コンテンツ署名用鍵 [Ksig] を生成し、ステップS
325において、生成したコンテンツ署名用鍵 [Ksig] を携帯情報端末13
15 0に送信する。

次に、コンテンツ配信サーバ150は、ステップS326において、携帯情報
端末130の秘密鍵 [K__SEC2__MBL] を適用してコンテンツ署名用鍵 [K
sig] を暗号化した暗号化鍵データ [E (K__SEC2__MBL, Ksig)]
を携帯情報端末130から受信する。

20 次に、コンテンツ配信サーバ150は、ステップS327において、先に生成
したコンテンツ署名用鍵 [Ksig] を適用して、ダウンロード対象のコンテン
ツ (M) に対する電子署名を行ない、署名されたコンテンツデータとしての [S
ig (Ksig, M)] を生成する。

次に、コンテンツ配信サーバ150は、ステップS328において、ダウンロ
ード先となるホームPC120に対して、署名されたコンテンツデータとしての
25 [Sig (Ksig, M)] と、先に携帯情報端末130から受信した暗号化鍵デ
ータ [E (K__SEC2__MBL, Ksig)] を送信する。

以上の処理が、携帯情報端末130からコンテンツダウンロード要求を受信し
た配信サーバ150の処理である。

次に、図14を参照して、コンテンツ配信サーバ150からコンテンツのダウンロードが実行されるホームPC120の処理について説明する。

ホームPC120は、ステップS331において、コンテンツ配信サーバ150から、署名されたコンテンツデータとしての $[Sig(K_{sig}, M)]$ と、暗号化鍵データ $[E(K_{SEC2_MBL}, K_{sig})]$ を受信する。

ステップS332において、ホームPC120は、自己の所有する携帯情報端末130の公開鍵 $[K_{PUB2_MBL}]$ を適用して、受信した暗号化鍵データ $[E(K_{SEC2_MBL}, K_{sig})]$ の復号処理を実行する。

ステップS333において、復号に失敗した場合は、ホームネットエリア共有秘密鍵 $[K_{sec}]$ が携帯情報端末130の有する鍵と異なるなど、正当なホームネットエリア共有秘密鍵でない可能性があり、ステップS337に進み、受信コンテンツを破棄する。

ステップS333において、復号に成功した場合は、復号によって取得したコンテンツ署名用鍵 $[K_{sig}]$ を適用して、署名されたコンテンツデータとしての $[Sig(K_{sig}, M)]$ の署名検証処理を実行する。この署名検証に不成功の場合(S335でNo)は、コンテンツ改竄の可能性があり、ステップS337に進み、受信コンテンツを破棄する。

署名検証に成功した場合(S335でYes)は、ステップS336において、受信コンテンツをホームPC120のストレージに格納し、ダウンロード処理を終了する。

以上の処理が、携帯情報端末130からコンテンツダウンロード要求を受信した配信サーバ150からのコンテンツを受信し、ダウンロードを実行するホームPC120の処理である。

上述したように、本実施例においては、コンテンツ配信サーバ150は、携帯情報端末130から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末130の送付してきたホームPCチケットに基づいて、ホームPC120が、携帯情報端末130の承認しているダウンロード先であることの確認が可能となる。すなわち、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテン

ダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームPCが、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本実施例においては、コンテンツ署名用鍵 [K s i g] を、携帯情報端末 130 の有する携帯情報端末 130 の秘密鍵 [K__S E C 2__M B L] により暗号化して、携帯情報端末 130 からコンテンツ配信サーバ 150 を介してダウンロード先であるホームPC 120 に送信し、ホームPC 120 において所有する携帯情報端末 130 の公開鍵 [K__P U B 2__M B L] により復号してコンテンツ署名用鍵 [K s i g] を取得する構成としたので、先に説明した処理例 1, 2 のようなホームネットエリア共有秘密鍵 [K s e c] を共有することなく、ホームネットエリア内でのみ共有される公開鍵、秘密鍵を所有する構成において、安全なコンテンツダウンロードが実行可能となる。

[コンテンツ配信処理例 4]

次に、コンテンツ配信処理例 4 について説明する。コンテンツ配信処理例 4 は、コンテンツ配信処理例 1, 2 で適用したホームネットエリア共有秘密鍵 [K s e c] を用いず、一般的な公開鍵方式における公開鍵と秘密鍵の一の鍵を適用した処理を実行する構成例であり、コンテンツ配信サーバ 150 がコンテンツのハッシュ値を算出して、ハッシュ値を携帯情報端末 130 が有する携帯情報端末 130 の秘密鍵 [K__S E C__M B L] で暗号化して、携帯情報端末 130 からコンテンツ配信サーバ 150 を介してダウンロード先であるホームPC 120 に送信する処理を実行する構成例である。

図 15 乃至図 18 を参照して、コンテンツ配信処理例 4 について説明する。図 15 は、コンテンツ配信サーバとコンテンツ配信サーバに対するアクセスを実行する携帯情報端末と、携帯情報端末からの要求に従って、コンテンツをダウンロードする大容量記憶媒体としてのホームストレージを備えたホームPC との 3 者間で実行する処理を示すシーケンス図である。図 16 は携帯情報端末の処理を示

すフローチャート、図 17 はコンテンツ配信サーバの処理を示すフローチャート、図 18 はホーム P C の処理を示すフローチャートである。

図 15 を参照して、本実施例の処理について説明する。図 15 において処理は、図に示す番号 (1) ~ (9) の順に進行する。

- 5 まず、(1) の処理として、携帯情報端末 130 は、コンテンツ配信サーバ 150 に対して、コンテンツのダウンロードを要求する。このダウンロード要求には、ダウンロード先となる機器、ここではホーム P C 120 から受領したホーム P C チケット [T i c k e t _ H S]、および、ダウンロード先となるホーム P C 120 の公開鍵を格納した公開鍵証明書 [K _ P U B _ H S - c e r t] が含まれる。
- 10 ホーム P C チケット [T i c k e t _ H S] は、ホーム P C 120 の ID [I D _ H S] と、携帯情報端末 130 の ID [I D _ M B L] と、ホーム P C 120 の公開鍵 [K _ P U B _ H S] をメッセージとして、該メッセージにホーム P C 120 の秘密鍵 [K _ S E C _ H S] で電子署名をしたデータ、すなわち、[S i g (K _ S E C _ H S , (I D _ H S , I D _ M B L , K _ P U B _ H S))] である。
- 15

- 携帯情報端末 130 からホーム P C チケット [S i g (K _ S E C _ M B L , (T i c k e t _ H S))]、ホーム P C 120 の公開鍵証明書 [K _ P U B _ H S - c e r t] を受信したコンテンツ配信サーバ 150 は、携帯情報端末 130 の公開鍵証明書から取得される携帯情報端末 130 の公開鍵を用いて、ホーム P C
- 20 チケット [S i g (K _ S E C _ M B L , (T i c k e t _ H S))] の署名検証を実行し、(2) の処理としてホーム P C チケット [T i c k e t _ H S] の検証処理を実行する。この検証処理の手順は、(a) ホーム P C 120 の公開鍵証明書 [K _ P U B _ H S - c e r t] の署名 (認証局署名) 検証による公開鍵証明書 [K _ P U B _ H S - c e r t] の正当性確認処理、(b) 正当性の確認された公開鍵
- 25 証明書 [K _ P U B _ H S - c e r t] からのホーム P C 120 の公開鍵 [K _ P U B _ H S] の取得処理、(c) 取得したホーム P C 120 の公開鍵 [K _ P U B _ H S] を適用したホーム P C チケット [T i c k e t _ H S]、すなわち、[S i g (K _ S E C _ H S , (I D _ H S , I D _ M B L , K _ P U B _ H S))] の署名検証処理である。

この手続き、すなわちホームPCチケット [Ticket_HS] の検証により、ホームPCチケット [Ticket_HS] が改竄の無い正当なチケットであることが確認されると、コンテンツ配信サーバ150は、(3)の処理として、コンテンツのハッシュ値 [H(M)] を計算する。次に、(4)の処理として、
5 コンテンツ配信サーバ150は、生成したコンテンツのハッシュ値 [H(M)] を携帯情報端末130に送信する。

コンテンツのハッシュ値 [H(M)] を受信した携帯情報端末130は、(5)の処理として、携帯情報端末130の第2の秘密鍵 [K_SEC2_MBL] を適用してコンテンツのハッシュ値 [H(M)] を暗号化して、暗号化ハッシュ値 [E(K_SEC2_MBL, H(M))]
10 (K_SEC2_MBL, H(M))] を生成し、(6)の処理として、生成した暗号化ハッシュ値 [E(K_SEC2_MBL, H(M))] をコンテンツ配信サーバ150に送信する。携帯情報端末130の第2秘密鍵 [K_SEC2_MBL] は、チケットで使用される公開鍵ペアとは別の第2の公開鍵ペアを構成する秘密鍵である。この第2の公開鍵ペアは、ホームネットエリア内のみで共有される秘密情報である。
15

(7)の処理として、コンテンツ配信サーバ150は、暗号化ハッシュ値 [E(K_SEC2_MBL, H(M))] とコンテンツ (M) からなるコンテンツパッケージ [M | E(K_SEC2_MBL, H(M))]
20 に対して、コンテンツパッケージ [M | E(K_SEC2_MBL, H(M))]
を送信する。

次に、コンテンツパッケージ [M | E(K_SEC2_MBL, H(M))] を受信したホームPC120は、(9)の処理として、自己の所有する携帯情報端末130の公開鍵 [K_PUB2_MBL] を適用して、受信したコンテンツパッケージ [M | E(K_SEC2_MBL, H(M))]
25 に含まれる暗号化ハッシュ値 [E(K_SEC2_MBL, H(M))] の復号処理を実行して、コンテンツ署名用鍵 [K_sig] を取り出して、コンテンツのハッシュ値 [H(M)] を取り出し、また、コンテンツ (M) に対するハッシュ値を計算して、両ハッシュ値の一致を確認する。一致している場合は、コンテンツの改竄がないと判定し、不

致の場合は、コンテンツ改竄ありと判定する。検証処理において、コンテンツ(M)のデータ改竄のないことが立証されたことを条件としてコンテンツの格納または再生処理を実行する。

次に、図16乃至図18のフローチャートを参照して、携帯情報端末130の
5 処理、コンテンツ配信サーバ150の処理、およびホームPC120の処理のそれぞれについて説明する。

まず、図16のフローチャートを参照して携帯情報端末130の処理手順について説明する。ステップS411において、携帯情報端末130は、ダウンロード先となる機器のデバイスチケット、ここではホームPC120のホームPCチケット[Ticket_HS]を含むデータをコンテンツ配信サーバ150に送信して、コンテンツのダウンロードを要求する。
10

ステップS412において、携帯情報端末130は、コンテンツ配信サーバ150の生成したコンテンツのハッシュ値[H(M)]を受信する。

ステップS413において、コンテンツのハッシュ値[H(M)]を受信した携帯情報端末130は、携帯情報端末130の第2の秘密鍵[K_SEC2_MBL]を適用してコンテンツのハッシュ値[H(M)]を暗号化して、暗号化ハッシュ値[E(K_SEC2_MBL, H(M))]を生成し、ステップS414において、生成した暗号化ハッシュ値[E(K_SEC2_MBL, H(M))]をコンテンツ配信サーバ150に送信する。
15

20 以上の処理が、携帯情報端末130とコンテンツ配信サーバ150間で実行されるコンテンツダウンロード要求処理における携帯情報端末130側の処理である。

次に、図17を参照して、携帯情報端末130からコンテンツダウンロード要求コマンドを受信するコンテンツ配信サーバ150の処理について説明する。

25 まず、コンテンツ配信サーバ150は、ステップS421において、携帯情報端末130から、ダウンロード先のデバイスチケット、ここではホームPC120のホームPCチケット[Ticket_HS]を含むデータをダウンロードコマンドとして受信する。

携帯情報端末130からホームPCチケット[Ticket_HS]を含むダ

ウンロードコマンドを受信したコンテンツ配信サーバ150は、ステップS422において、ホームPCチケット[Ticket_HS]の検証処理を実行する。この検証処理は、先に説明したと同様の処理である。

5 ステップS423において、チケット検証が不成立と判定された場合は、チケット、すなわちホームPCチケット[Ticket_HS]が偽造されたものである可能性があり、ステップS429に進み、エラーメッセージを携帯情報端末130に送信して処理を終了する。この場合は、コンテンツのダウンロード処理は実行されない、

10 ステップS423において、チケット検証が成立したと判定された場合は、ステップS424に進み、コンテンツのハッシュ値[H(M)]を生成し、ステップS425において、生成したコンテンツのハッシュ値[H(M)]を携帯情報端末130に送信する。

15 次に、コンテンツ配信サーバ150は、ステップS426において、携帯情報端末130の秘密鍵[K_SEC2_MBL]を適用してコンテンツのハッシュ値[H(M)]を暗号化した暗号化ハッシュ値[E(K_SEC2_MBL, H(M))]を携帯情報端末130から受信する。

20 次に、コンテンツ配信サーバ150は、ステップS427において、携帯情報端末130から受信した暗号化ハッシュ値[E(K_SEC2_MBL, H(M))]とコンテンツ(M)からなるコンテンツパッケージ[M | E(K_SEC2_MBL, H(M))]を生成する。

次に、コンテンツ配信サーバ150は、ステップS428において、ダウンロード先となるホームPC120に対して、コンテンツパッケージ[M | E(K_SEC2_MBL, H(M))]を送信する。

25 以上の処理が、携帯情報端末130からコンテンツダウンロード要求を受信した配信サーバ150の処理である。

次に、図18を参照して、コンテンツ配信サーバ150からコンテンツのダウンロードが実行されるホームPC120の処理について説明する。

ホームPC120は、ステップS431において、コンテンツ配信サーバ150から、コンテンツパッケージ[M | E(K_SEC2_MBL, H(M))]を

受信する。

- ステップ S 4 3 2 において、ホーム P C 1 2 0 は、自己の所有する携帯情報端末 1 3 0 の公開鍵 [K__P U B 2 __M B L] を適用して、受信したコンテンツパッケージ [M | E (K__S E C 2 __M B L, H (M))] に含まれる暗号化ハッシュ値 [E (K__S E C 2 __M B L, H (M))] の復号処理を実行する。

ステップ S 4 3 3 において、復号に失敗した場合は、自己の所有する携帯情報端末 1 3 0 の公開鍵 [K__P U B 2 __M B L] が携帯情報端末 1 3 0 の有する秘密鍵に対するペアと異なるなど、正当な公開鍵でない可能性があり、ステップ S 4 3 7 に進み、受信コンテンツを破棄する。

- 10 ステップ S 4 3 3 において、復号に成功した場合は、復号によって取得したコンテンツのハッシュ値 [H (M)] と、コンテンツ (M) に基づいて計算により算出したハッシュ値 H (M)' との比較を実行する。この比較において両ハッシュ値が不一致の場合 (S 4 3 5 で N o) は、コンテンツ改竄の可能性があり、ステップ S 4 3 7 に進み、受信コンテンツを破棄する。
- 15 両ハッシュ値が一致した場合 (S 4 3 5 で Y e s) は、ステップ S 4 3 6 において、受信コンテンツをホーム P C 1 2 0 のストレージに格納し、ダウンロード処理を終了する。

- 以上の処理が、携帯情報端末 1 3 0 からコンテンツダウンロード要求を受信した配信サーバ 1 5 0 からのコンテンツを受信し、ダウンロードを実行するホーム P C 1 2 0 の処理である。

- 20 上述したように、本実施例においては、コンテンツ配信サーバ 1 5 0 は、携帯情報端末 1 3 0 から受信したコンテンツダウンロード先のデバイスチケットの検証が可能となり、携帯情報端末 1 3 0 の送付してきたホーム P C チケットに基づいて、ホーム P C 1 2 0 が、携帯情報端末 1 3 0 の承認しているダウンロード先であることの確認が可能となる。すなわち、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先のデバイスによる署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホーム P C が、携帯情報端末の承認しているダウンロード先である確認が可

能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本実施例においては、コンテンツのハッシュ値 [H (M)] を、携帯情報端末 1 3 0 の第 2 の秘密鍵 [K __ S E C 2 __ M B L] により暗号化して、携帯情報
5 報端末 1 3 0 からコンテンツ配信サーバ 1 5 0 を介してダウンロード先であるホーム P C 1 2 0 に送信し、ホーム P C 1 2 0 において所有する携帯情報端末 1 3 0 の公開鍵 [K __ P U B 2 __ M B L] により復号してコンテンツのハッシュ値 [H (M)] を取得して、コンテンツに基づいてみずから算出するハッシュ値と比較する構成としたので、先に説明した処理例 1 , 2 のようなホームネットエリア共有
10 秘密鍵 [K s e c] を共有することなく、ホームネットエリア内でのみ共有される公開鍵、秘密鍵を所有する構成において、安全なコンテンツダウンロードが実行可能となる。

[情報処理装置およびサーバ構成例]

15 次に本システムを構成するホーム P C 1 2 0、携帯情報端末 1 3 0 としての情報処理装置、およびコンテンツ配信サーバ 1 5 0 の構成例について図 1 9、図 2 0 を用いて説明する。図 1 9 には、ホーム P C 1 2 0、携帯情報端末 1 3 0 としての情報処理装置の構成例を示す。

C P U (Central processing Unit) 5 0 1 は、各種アプリケーションプログラム
20 や、O S (Operating System) を実行する演算ユニットである。R O M (Read-Only-Memory) 5 0 2 は、C P U 5 0 1 が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。R A M (Random Access Memory) 5 0 3 は、C P U 5 0 1 の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用さ
25 れる。

ホストバス 5 0 4 はブリッジ 5 0 5 を介して P C I (Peripheral Component Internet/Interface) バスなどの外部バス 5 0 6 に接続されている。

キーボード 5 0 8 は C P U 5 0 1 に各種の指令を入力するためにユーザにより操作され、ポインティングデバイス 5 0 9 はディスプレイ 5 1 0 の画面上の位置

指定、コマンド指定などの際にユーザによって操作される。ディスプレイ 510 は例えば CRT、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。HDD (Hard Disk Drive) 511 は、情報記憶媒体としてのハードディスクを駆動し、ハードディスクからのプログラム、データの読み取り
5 またはハードディスクに対するプログラム、データの書き込みを実行する。

ドライブ 512 は、フロッピーディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体 513 の記録再生を実行するドライブであり、各リムーバブル記録媒体 513 からのプログラムまたはデ
10 ータ再生、リムーバブル記録媒体 513 に対するプログラムまたはデータ格納を実行する。

各記憶媒体に記録されたプログラムまたはデータを読み出して CPU 501 において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース 507、外部バス 506、ブリッジ 505、ホストバス 504 を介して
15 例えば接続されている RAM 503 に供給する。

キーボード 508 乃至ドライブ 512 はインタフェース 507 に接続されており、インタフェース 507 は外部バス 506、ブリッジ 505、およびホストバス 504 を介して CPU 501 に接続されている。

通信部 514 は情報処理装置の接続されたルータ等を介してサーバー装置と通
20 信し、CPU 501、HDD 511 等から供給されたデータをパケット化して送信したり、ルータを介してパケットを受信する処理を実行する。通信部 503 は外部バス 506、ブリッジ 505、およびホストバス 504 を介して CPU 501 に接続されている。

次に、コンテンツ配信処理を実行するサーバー装置の構成について図 20 を参
25 照して説明する。

CPU (Central processing Unit) 701 は、各種アプリケーションプログラムや、OS (Operating System) を実行する演算ユニットである。ROM (Read-Only-Memory) 702 は、CPU 701 が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM (Random Access Memory)

703は、CPU701の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

ドライブ705は、フロッピーディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical)ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体706の記録再生を実行するドライブであり、各リムーバブル記録媒体706からのプログラムまたはデータ再生、リムーバブル記録媒体706に対するプログラムまたはデータ格納を実行する。各記憶媒体に記録されたプログラムまたはデータを読み出してCPU701において実行または処理を行なう場合は、読み出したプログラム、データはバス704を介して例えば接続されているRAM703、通信部707に供給される。

通信部707は、PC、携帯情報端末等の通信端末との通信部であり、CPU701のデータ処理によって生成したパケットの送信したり、インターネットを介してパケットを受信する処理を実行する。

CPU701乃至通信部707はバス704によって相互接続され、データの転送が可能な構成となっている。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only

Memory)に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなりムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなりムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

産業上の利用可能性

以上説明してきたように、本発明の構成によれば、コンテンツ配信サーバは、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツダウンロード先の装置による署名のなされたチケットを受信して、チケットを検証することにより、コンテンツダウンロード先としての情報処理装置、例えばホームPCが、携帯情報端末の承認しているダウンロード先である確認が可能となり、ダウンロード先の機器との直接認証を行なうことなく、ダウンロード先の機器の正当性確認が可能となる。

また、本発明の一実施例構成によれば、コンテンツ署名用鍵 [K s i g] を、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置と、コンテンツダウンロード先としての情報処理装置、例えばホームPCとの共有するホームネットエリア共有秘密鍵 [K s e c] により暗号化して、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置からコンテンツ配

信サーバを介してダウンロード先である情報処理装置、例えばホームP Cに送信し、ホームP Cにおいて所有するホームネットエリア共有秘密鍵 [K s e c] により復号してコンテンツ署名用鍵 [K s i g] を取得する構成としたので、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置と、コンテンツダウンロード先としての情報処理装置、例えばホームP Cとが同一のホームネットエリア共有秘密鍵 [K s e c] を有することが、ダウンロード先であるホームP Cにおいてコンテンツ署名用鍵 [K s i g] を取得できる条件となり、同一のホームネットエリア共有秘密鍵 [K s e c] を有する機器間においてのみ、有効なコンテンツの検証、ダウンロードが実行可能となり、不正コンテンツの格納を防止することが可能となる。

また、本発明の一実施例構成によれば、コンテンツのハッシュ値 [H (M)] を、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置と、コンテンツダウンロード先としての情報処理装置、例えばホームP Cとが共有するホームネットエリア共有秘密鍵 [K s e c] により暗号化して、コンテンツダウンロード要求を行なう例えば携帯情報端末等の情報処理装置から、コンテンツ配信サーバを介して、コンテンツダウンロード先としての情報処理装置、例えばホームP Cに送信し、ホームP Cにおいて所有するホームネットエリア共有秘密鍵 [K s e c] により復号してコンテンツのハッシュ値 [H (M)] を取得して、コンテンツに基づいてみずから算出するハッシュ値と比較する構成としたので、同一のホームネットエリア共有秘密鍵 [K s e c] を有する機器間においてのみ、有効なコンテンツの検証、ダウンロードが実行可能となり、不正コンテンツの格納を防止することが可能となる。

また、本発明の一実施例構成によれば、コンテンツ署名用鍵 [K s i g]、あるいはコンテンツのハッシュ値 [H (M)] を、コンテンツダウンロード要求を行なう例えば携帯情報端末の秘密鍵 [K __ S E C __ M B L] により暗号化して、携帯情報端末からコンテンツ配信サーバを介してダウンロード先であるホームP Cに送信し、ホームP Cにおいて所有する携帯情報端末の公開鍵 [K __ P U B __ M B L] により復号してコンテンツ署名用鍵 [K s i g]、あるいはコンテンツのハッシュ値 [H (M)] を取得して、コンテンツの検証を実行する構成としたので、ホ

ームネットエリア共有秘密鍵 [K s e c] を共有することなく、通常の公開鍵方式の公開鍵、秘密鍵を所有する構成において、セキュアなコンテンツダウンロード処理が実行可能となる。

請求の範囲

1. 自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行

5 する第1の情報処理装置と、

コンテンツのダウンロード先として指定される第2の情報処理装置と、

前記第1の情報処理装置からのコンテンツダウンロード要求を受信して、前記第2の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有し、

10 前記第1の情報処理装置は、

前記第2の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信サーバに送信する処理を実行し、

前記コンテンツ配信サーバは、

前記チケットの電子署名の検証を実行し、該検証に成功したことを条件として、

15 前記第2の情報処理装置が前記第1の情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第2の情報処理装置に対するコンテンツ送信を実行する構成を有することを特徴とするコンテンツ配信システム。

2. 前記第1の情報処理装置と、前記第2の情報処理装置は、共有する秘密鍵
20 としてのホームネットエリア共有秘密鍵 [K s e c] を有し、

前記第1の情報処理装置は、

前記ホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K s e c, K s i g)] を、コンテンツ配信サーバを介して第2の情報
25 処理装置に送信する処理を実行し、

前記第2の情報処理装置は、

前記ホームネットエリア共有秘密鍵 [K s e c] による暗号化鍵データ [E (K s e c, K s i g)] の復号により取得したコンテンツ署名用鍵 [K s i g] を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行する構

成であることを特徴とする請求項 1 に記載のコンテンツ配信システム。

3. 前記第 1 の情報処理装置と、前記第 2 の情報処理装置は、共有する秘密鍵とし

5 でのホームネットエリア共有秘密鍵 [K s e c] を有し、

前記第 1 の情報処理装置は、

前記ホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ
配信サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化
ハッシュ値 [E (K s e c, H (M))] を、コンテンツ配信サーバを介して第

10 2 の情報処理装置に送信する処理を実行し、

前記第 2 の情報処理装置は、

前記ホームネットエリア共有秘密鍵 [K s e c] による暗号化ハッシュ値 [E
(K s e c, H (M))] の復号により取得したコンテンツのハッシュ値 [H (M)]
を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成

15 であることを特徴とする請求項 1 に記載のコンテンツ配信システム。

4. 前記第 1 の情報処理装置と、前記第 2 の情報処理装置は、それぞれ公開鍵
暗号方式の公開鍵、秘密鍵を有し、

前記第 1 の情報処理装置は、

20 該第 1 の情報処理装置の秘密鍵 [K _ S E C _ M B L] を適用して、前記コン
テンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号
化鍵データ [E (K _ S E C _ M B L, K s i g)] を、コンテンツ配信サーバ
を介して第 2 の情報処理装置に送信する処理を実行し、

前記第 2 の情報処理装置は、

25 前記第 1 の情報処理装置の公開鍵 [K _ P U B _ M B L] による暗号化鍵デー
タ [E (K _ S E C _ M B L, K s i g)] の復号により取得したコンテンツ署
名用鍵 [K s i g] を適用して、コンテンツ配信サーバからの受信コンテンツの
署名検証を実行する構成であることを特徴とする請求項 1 に記載のコンテンツ配
信システム。

5. 前記第1の情報処理装置と、前記第2の情報処理装置は、それぞれ公開鍵暗号方式の公開鍵、秘密鍵を有し、

前記第1の情報処理装置は、

- 5 該第1の情報処理装置の秘密鍵 $[K_SEC_MBL]$ を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値 $[H(M)]$ を暗号化した暗号化ハッシュ値 $[E(K_SEC_MBL, H(M))]$ を、コンテンツ配信サーバを介して第2の情報処理装置に送信する処理を実行し、

前記第2の情報処理装置は、

- 10 前記第1の情報処理装置の公開鍵 $[K_PUB_MBL]$ による暗号化ハッシュ値 $[E(K_SEC_MBL, H(M))]$ の復号により取得したコンテンツのハッシュ値 $[H(M)]$ を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行する構成であることを特徴とする請求項1に記載のコンテンツ配信システム。

15

6. 前記チケットは、前記第1の情報処理装置と、前記第2の情報処理装置各々の識別子 (ID) を含むデータに対して、前記第2の情報処理装置の秘密鍵による電子署名がなされたチケットであり、

前記コンテンツ配信サーバは、

- 20 前記第2の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証を実行する構成であることを特徴とする請求項1に記載のコンテンツ配信システム。

7. 前記コンテンツ配信サーバは、

- 25 前記チケットの電子署名の検証処理として、以下の処理

(a) 前記第2の情報処理装置の公開鍵証明書署名 (認証局署名) 検証による公開鍵証明書の正当性確認処理、

(b) 正当性の確認された公開鍵証明書からの前記第2の情報処理装置の公開鍵の取得処理、

(c) 取得した前記第2の情報処理装置の公開鍵を適用した前記第2の情報処理装置のチケットの署名検証処理、

の各処理を実行する構成であることを特徴とする請求項1に記載のコンテンツ配信システム。

5

8. 自装置と異なるダウンロード先を指定したコンテンツダウンロード要求を実行する第1の情報処理装置と、コンテンツのダウンロード先として指定される第2の情報処理装置と、前記第1の情報処理装置からのコンテンツダウンロード要求を受信して、前記第2の情報処理装置に対するコンテンツの送信処理を実行するコンテンツ配信サーバとを有するコンテンツ配信システムにおけるコンテンツ配信方法であり、

10

前記第1の情報処理装置において、

前記第2の情報処理装置の電子署名がなされたチケットを前記コンテンツ配信サーバに送信するステップと、

15

前記コンテンツ配信サーバにおいて、

前記チケットの電子署名の検証を実行するステップと、

前記検証に成功したことを条件として、前記第2の情報処理装置が前記第1の情報処理装置の承認したコンテンツダウンロード先であると判定して、前記第2の情報処理装置に対するコンテンツ送信を実行するステップと、

20

を有することを特徴とするコンテンツ配信方法。

9. 前記コンテンツ配信方法において、

前記第1の情報処理装置は、

前記第1の情報処理装置と、前記第2の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K s e c, K s i g)] を、コンテンツ配信サーバを介して第2の情報処理装置に送信する処理を実行し、

25

前記第2の情報処理装置は、

前記ホームネットエリア共有秘密鍵 [K s e c] による暗号化鍵データ [E (K s e c, K s i g)] の復号により取得したコンテンツ署名用鍵 [K s i g] を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行することを特徴とする請求項 8 に記載のコンテンツ配信方法。

5

1 0 . 前記コンテンツ配信方法において、

前記第 1 の情報処理装置は、

前記第 1 の情報処理装置と、前記第 2 の情報処理装置の共有する秘密鍵としてのホームネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信
10 サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E (K s e c, H (M))] を、コンテンツ配信サーバを介して第 2 の情報処理装置に送信する処理を実行し、

前記第 2 の情報処理装置は、

前記ホームネットエリア共有秘密鍵 [K s e c] による暗号化ハッシュ値 [E
15 (K s e c, H (M))] の復号により取得したコンテンツのハッシュ値 [H (M)] を適用して、コンテンツ配信サーバからの受信コンテンツの検証を実行することを特徴とする請求項 8 に記載のコンテンツ配信方法。

1 1 . 前記コンテンツ配信方法において、

20 前記第 1 の情報処理装置は、

該第 1 の情報処理装置の秘密鍵 [K __ S E C __ M B L] を適用して、前記コンテンツ配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K __ S E C __ M B L, K s i g)] を、コンテンツ配信サーバを介して第 2 の情報処理装置に送信する処理を実行し、

25 前記第 2 の情報処理装置は、

前記第 1 の情報処理装置の公開鍵 [K __ P U B __ M B L] による暗号化鍵データ [E (K __ S E C __ M B L, K s i g)] の復号により取得したコンテンツ署名用鍵 [K s i g] を適用して、コンテンツ配信サーバからの受信コンテンツの署名検証を実行することを特徴とする請求項 8 に記載のコンテンツ配信方法。

1 2 . 前記コンテンツ配信方法において、

前記第 1 の情報処理装置は、

該第 1 の情報処理装置の秘密鍵 [K _ S E C _ M B L] を適用して、前記コン
5 テンツ配信サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した
暗号化ハッシュ値 [E (K _ S E C _ M B L , H (M))] を、コンテンツ配信
サーバを介して第 2 の情報処理装置に送信する処理を実行し、

前記第 2 の情報処理装置は、

前記第 1 の情報処理装置の公開鍵 [K _ P U B _ M B L] による暗号化ハッシ
10 ュ値 [E (K _ S E C _ M B L , H (M))] の復号により取得したコンテンツ
のハッシュ値 [H (M)] を適用して、コンテンツ配信サーバからの受信コンテ
ンツの検証を実行することを特徴とする請求項 8 に記載のコンテンツ配信方法。

1 3 . 前記チケットは、前記第 1 の情報処理装置と、前記第 2 の情報処理装置
15 各々の識別子 (I D) を含むデータに対して、前記第 2 の情報処理装置の秘密鍵
による電子署名がなされたチケットであり、

前記コンテンツ配信サーバは、

前記第 2 の情報処理装置の公開鍵を適用して、前記チケットの電子署名の検証
を実行することを特徴とする請求項 8 に記載のコンテンツ配信方法。

20

1 4 . 前記コンテンツ配信サーバは、

前記チケットの電子署名の検証処理として、

(a) 前記第 2 の情報処理装置の公開鍵証明書 of 署名 (認証局署名) 検証によ
る公開鍵証明書の正当性確認処理、

25 (b) 正当性の確認された公開鍵証明書からの前記第 2 の情報処理装置の公開
鍵の取得処理、

(c) 取得した前記第 2 の情報処理装置の公開鍵を適用した前記第 2 の情報処
理装置のチケットの署名検証処理、

の各処理を実行することを特徴とする請求項 8 に記載のコンテンツ配信方法。

15. 自装置と異なるダウンロード先を指定したコンテンツダウンロード要求
を実行する情報処理装置であり、

コンテンツのダウンロード先の第2の情報処理装置の電子署名がなされたチケ
5 ットを格納した記憶手段と、

前記記憶手段に格納した前記チケットを含むコンテンツダウンロード要求コマ
ンドを生成する制御手段と、

前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サ
ーバに対して送信する通信手段と、

10 を有することを特徴とする情報処理装置。

16. 前記情報処理装置の制御手段は、

該情報処理装置と、前記第2の情報処理装置の共有する秘密鍵としてのホーム
ネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信サーバの
15 生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵データ [E (K
s e c, K s i g)] を、前記第2の情報処理装置に対する送信データとして生
成する構成を有することを特徴とする請求項15に記載の情報処理装置。

17. 前記情報処理装置の制御手段は、

20 該情報処理装置と、前記第2の情報処理装置の共有する秘密鍵としてのホーム
ネットエリア共有秘密鍵 [K s e c] を適用して、前記コンテンツ配信サーバの
生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E
(K s e c, H (M))] を、前記第2の情報処理装置に対する送信データとし
て生成する構成を有することを特徴とする請求項15に記載の情報処理装置。

25

18. 前記情報処理装置の制御手段は、

該情報処理装置の秘密鍵 [K __ S E C __ M B L] を適用して、前記コンテンツ
配信サーバの生成したコンテンツ署名用鍵 [K s i g] を暗号化した暗号化鍵デ
ータ [E (K __ S E C __ M B L, K s i g)] を、前記第2の情報処理装置に対

する送信データとして生成する構成を有することを特徴とする請求項 15 に記載の情報処理装置。

19. 前記情報処理装置の制御手段は、

- 5 該情報処理装置の秘密鍵 [K__SEC__MBL] を適用して、前記コンテンツ配信サーバの生成したコンテンツのハッシュ値 [H (M)] を暗号化した暗号化ハッシュ値 [E (K__SEC__MBL, H (M))] を、前記第 2 の情報処理装置に対する送信データとして生成する構成を有することを特徴とする請求項 15 に記載の情報処理装置。

10

20. 自装置と異なるダウンロード先を指定したコンテンツダウンロード要求処理を実行するコンピュータ・プログラムであり、

コンテンツのダウンロード先の第 2 の情報処理装置の電子署名がなされたチケットを取得するステップと、

- 15 前記チケットを含むコンテンツダウンロード要求コマンドを生成するステップと、

前記チケットを含むコンテンツダウンロード要求コマンドをコンテンツ配信サーバに対して送信するステップと、

を有することを特徴とするコンピュータ・プログラム。

20

21. コンテンツの送信処理を実行するコンピュータ・プログラムであり、

第 1 の情報処理装置から自装置と異なるダウンロード先として第 2 の情報処理装置を指定したコンテンツダウンロード要求処理を受信するステップと、

- 25 前記コンテンツダウンロード要求に含まれるダウンロード先の第 2 の情報処理装置の電子署名がなされたチケットに含まれる電子署名検証処理を実行するステップと、

前記検証に成功したことを条件として、前記第 2 の情報処理装置に対するコンテンツ送信を実行するステップと、

を有することを特徴とするコンピュータ・プログラム。

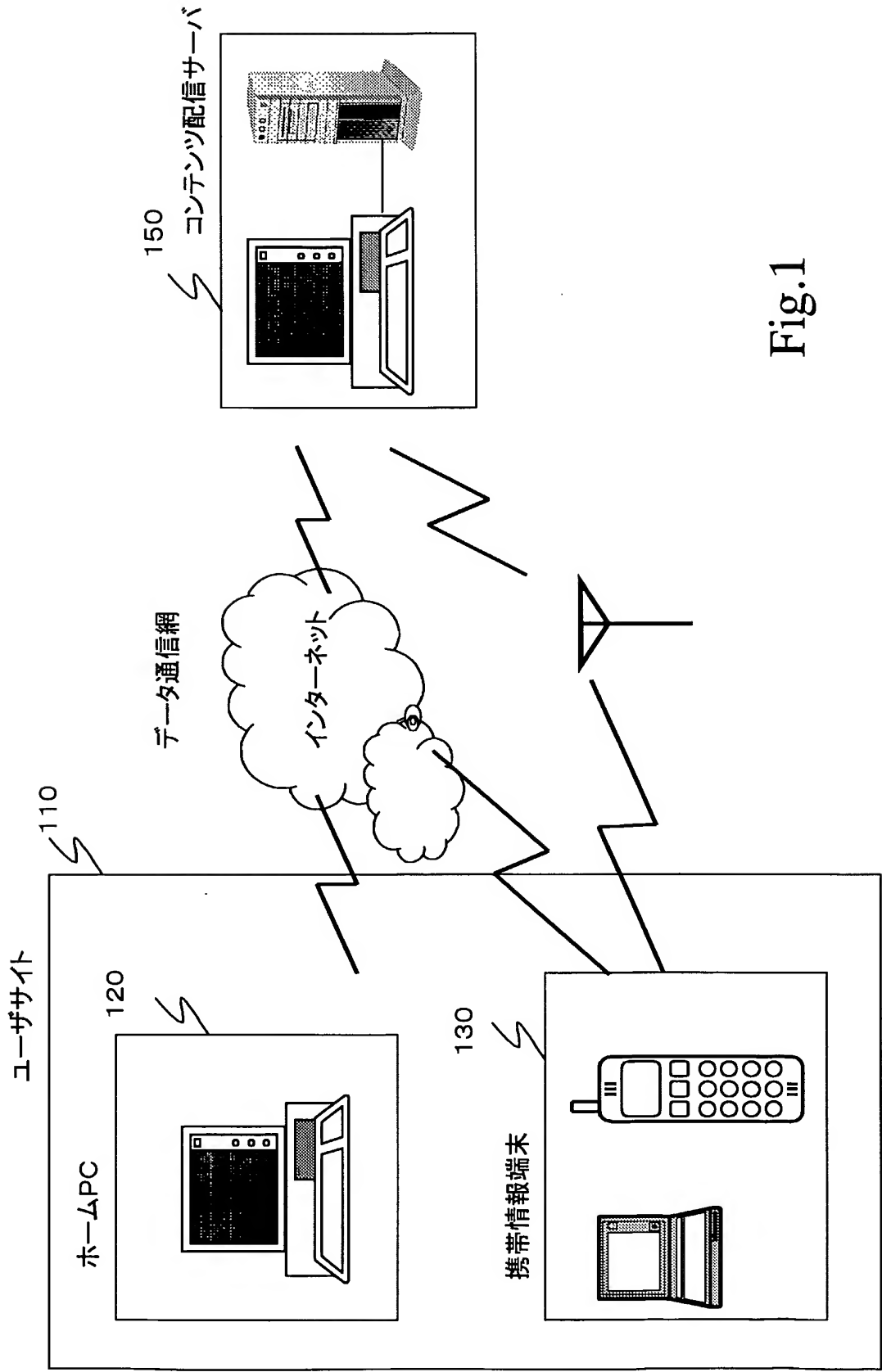
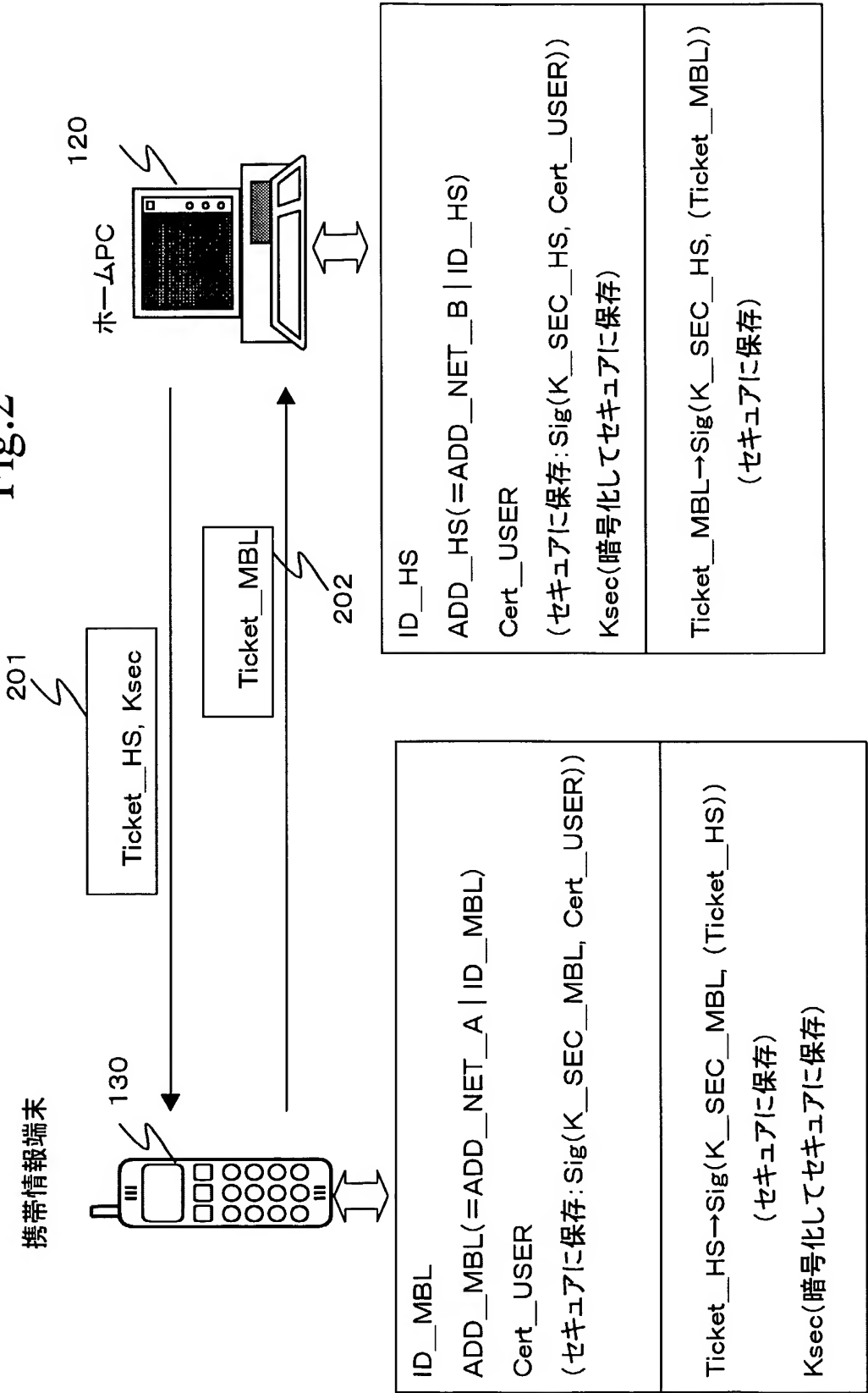
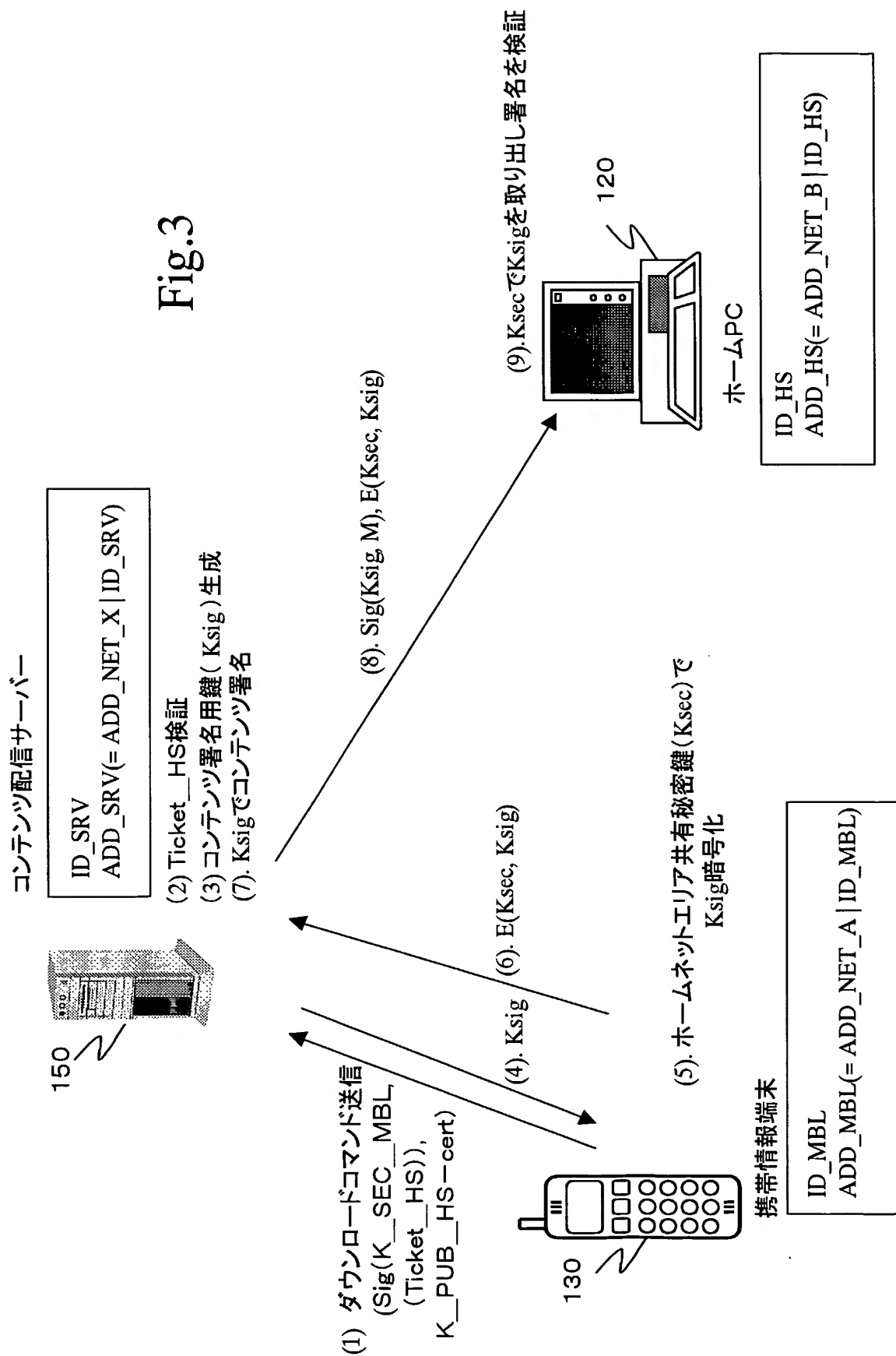


Fig.1

Fig.2



3/20



4/20

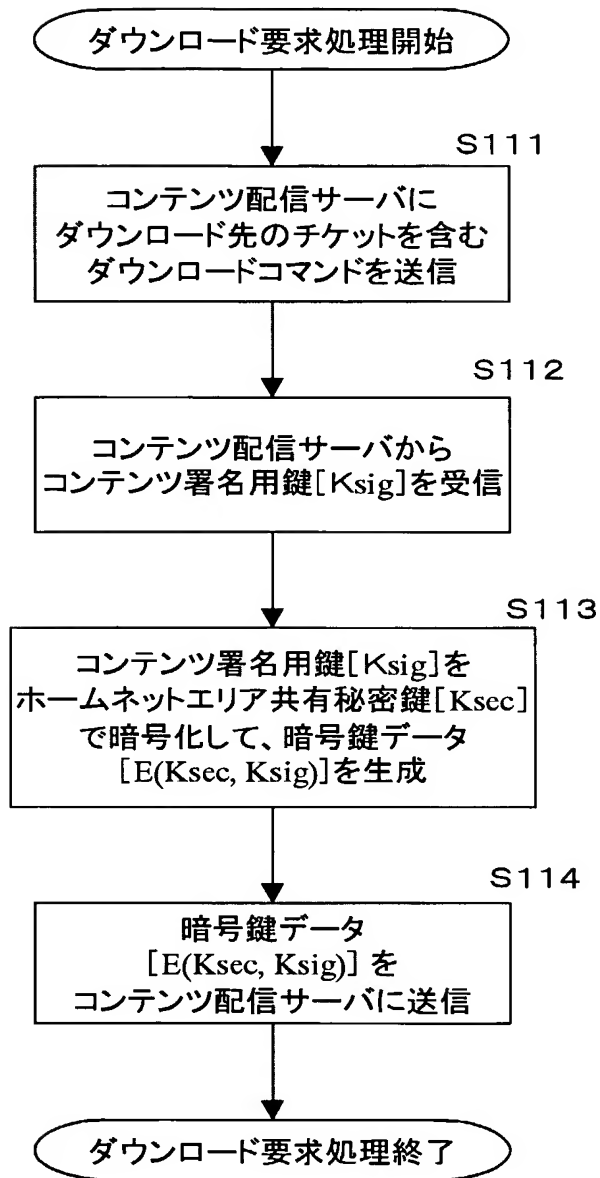
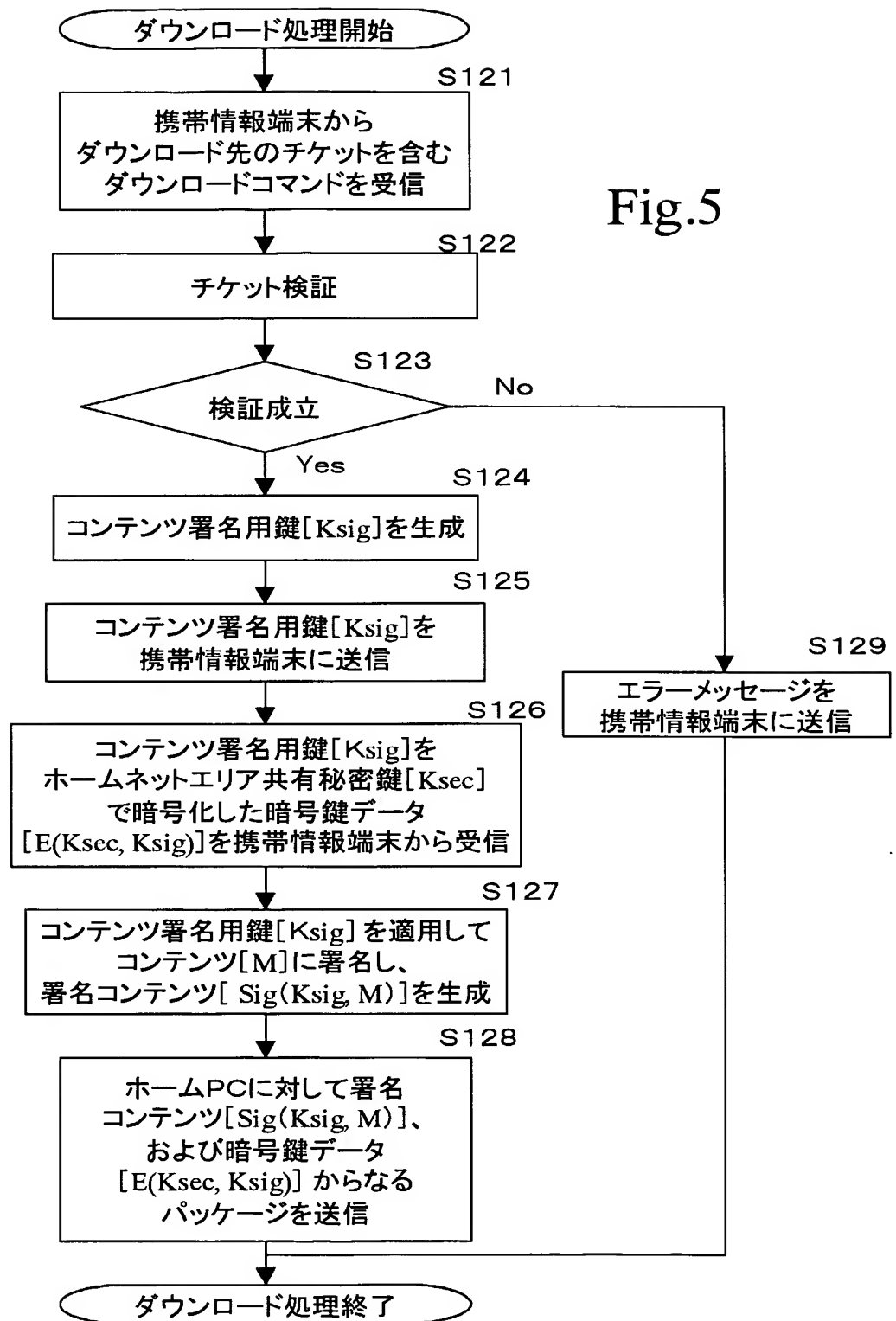
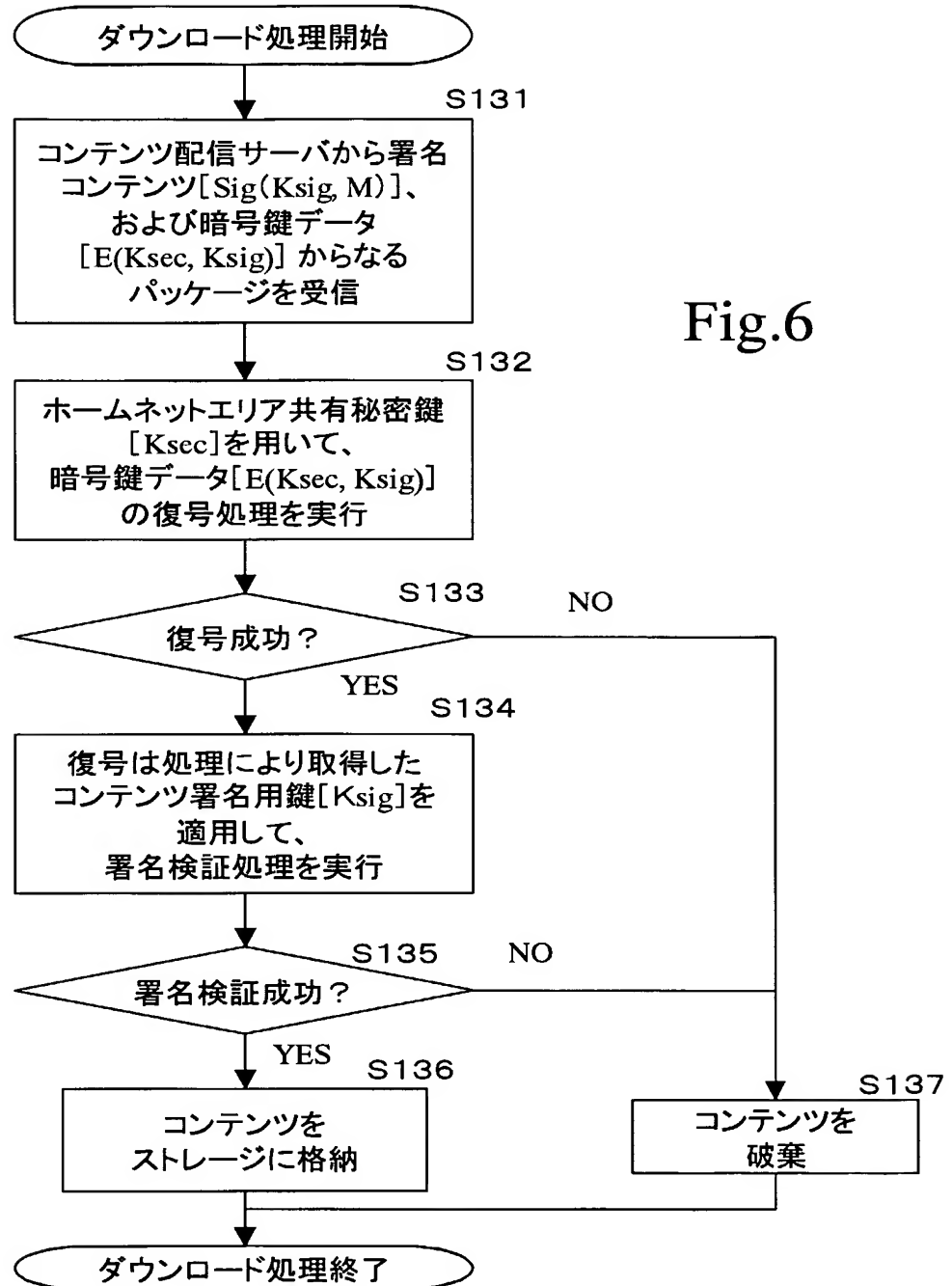


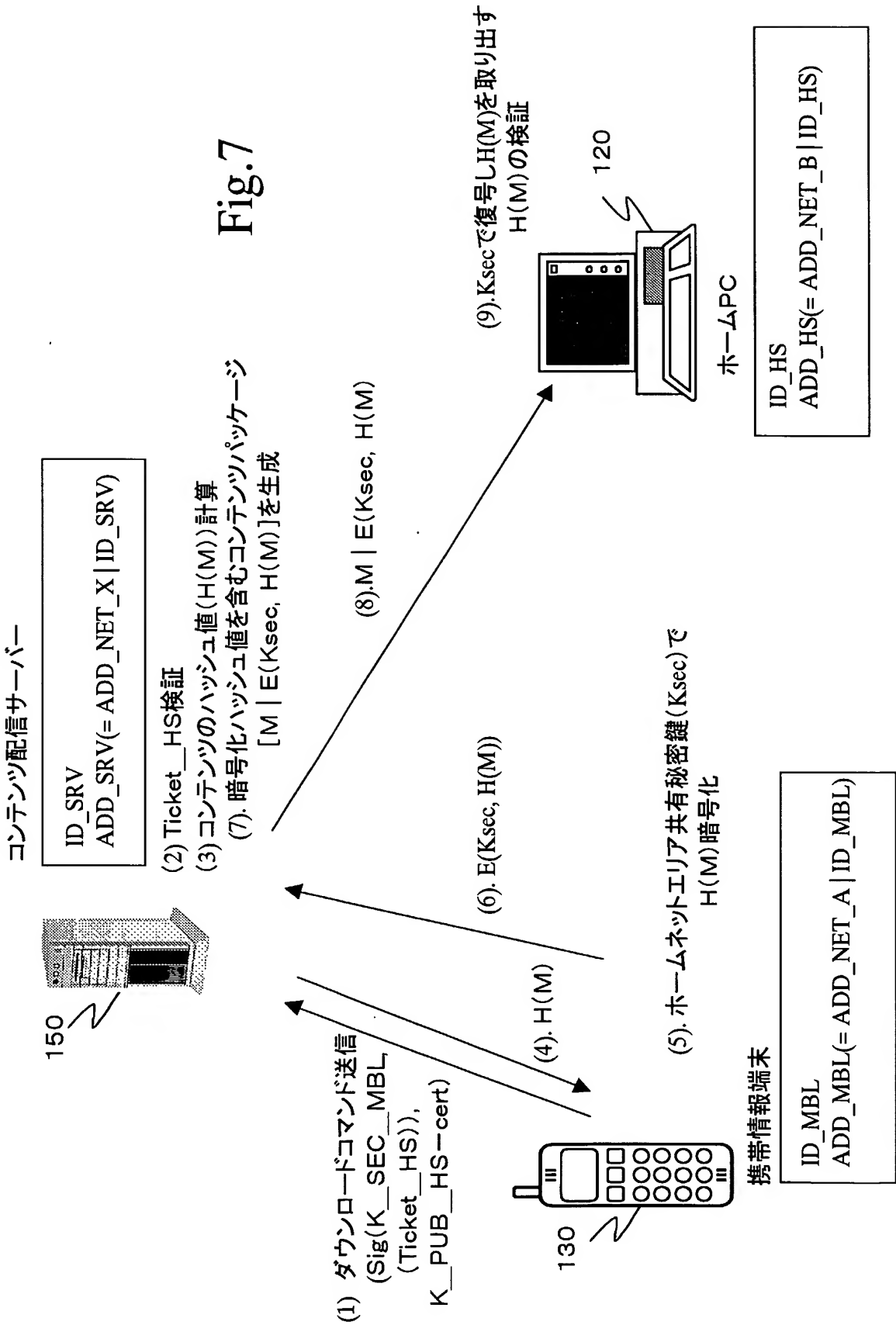
Fig.4

5/20



6/20





8/20

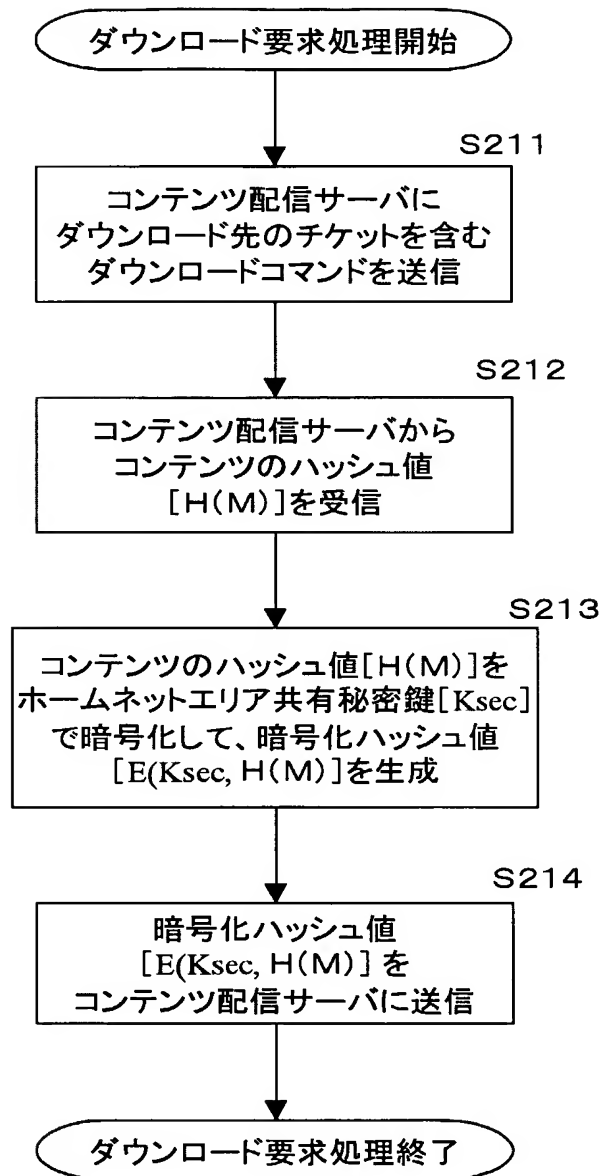
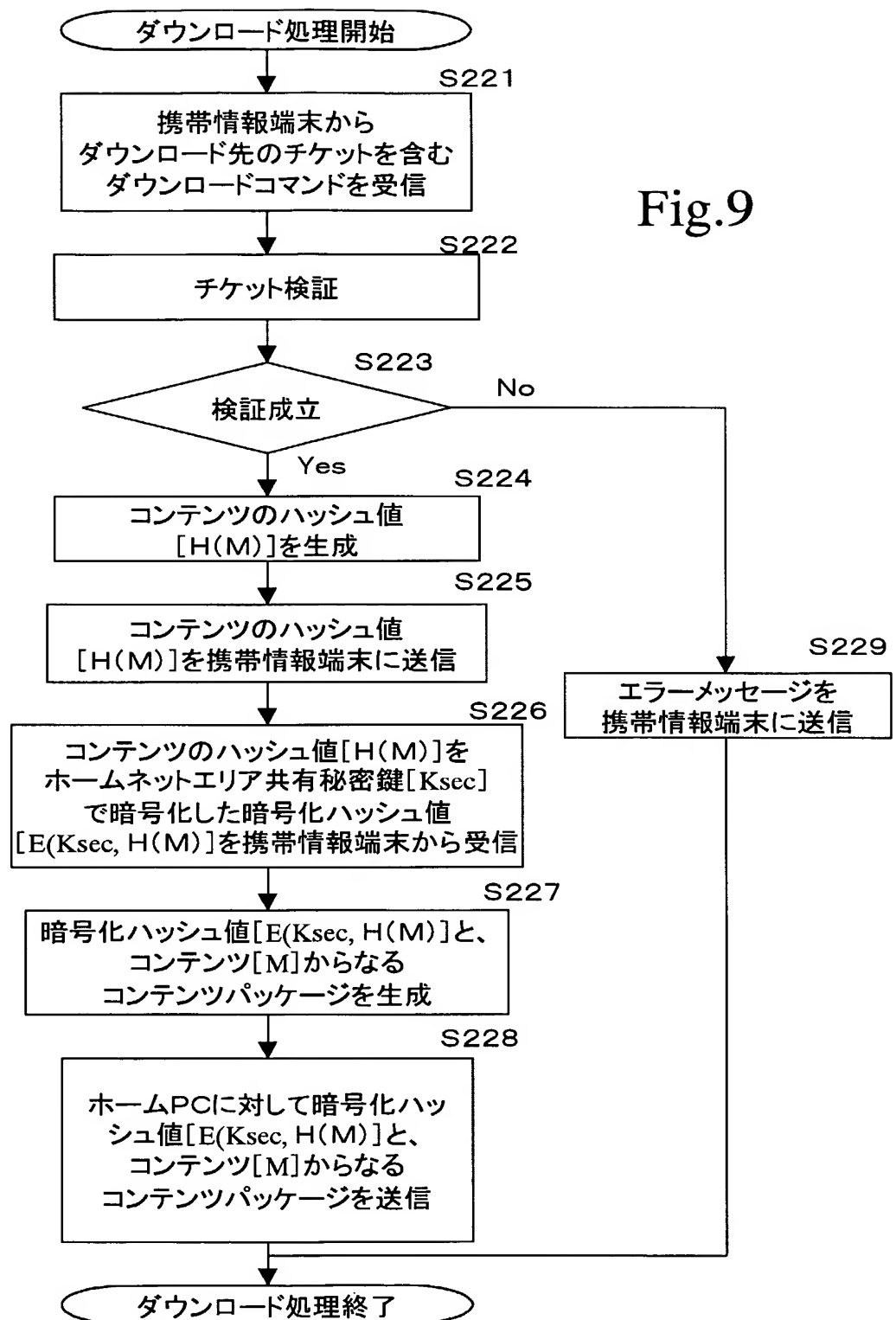


Fig.8

9/20



10/20

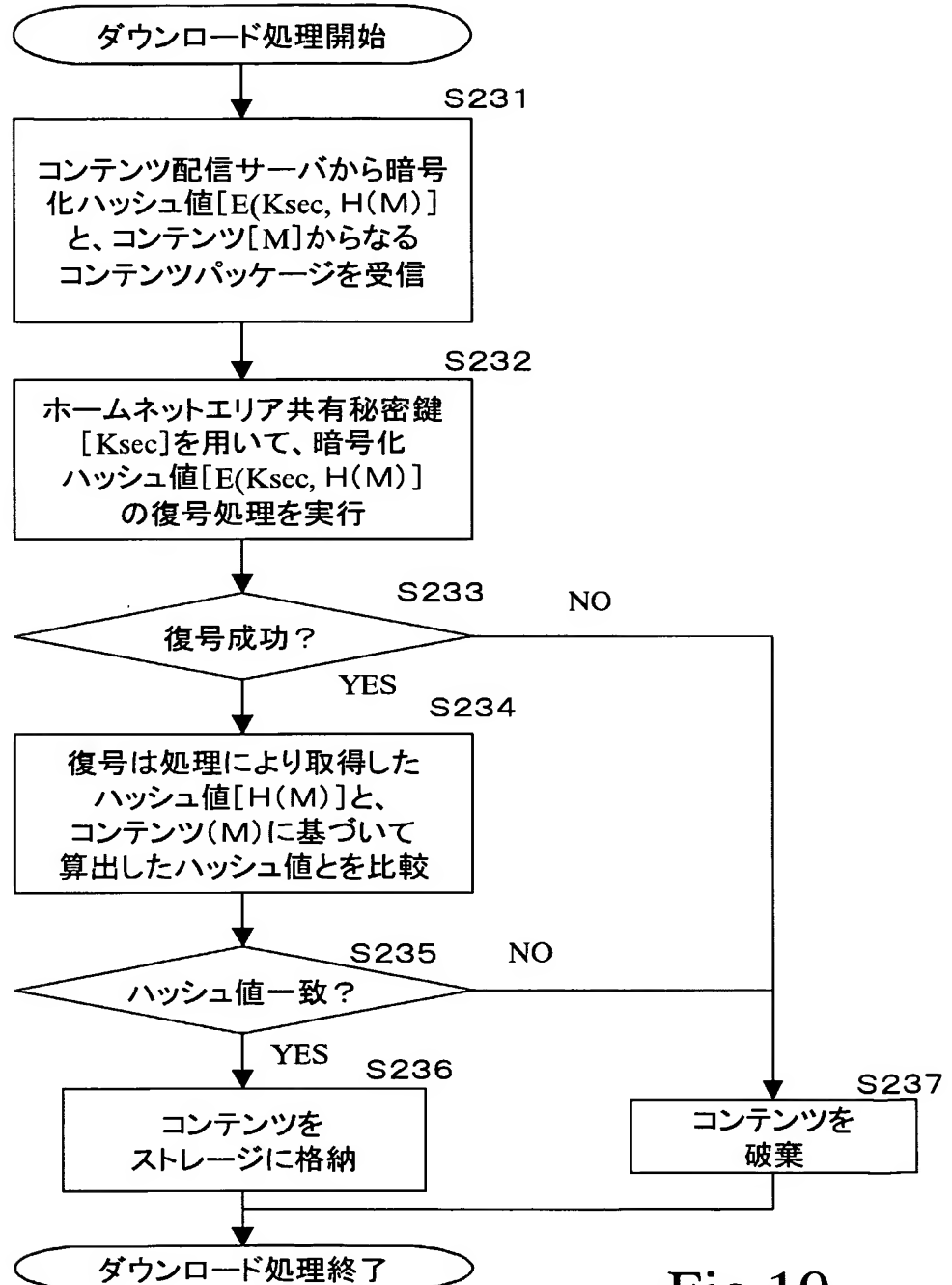
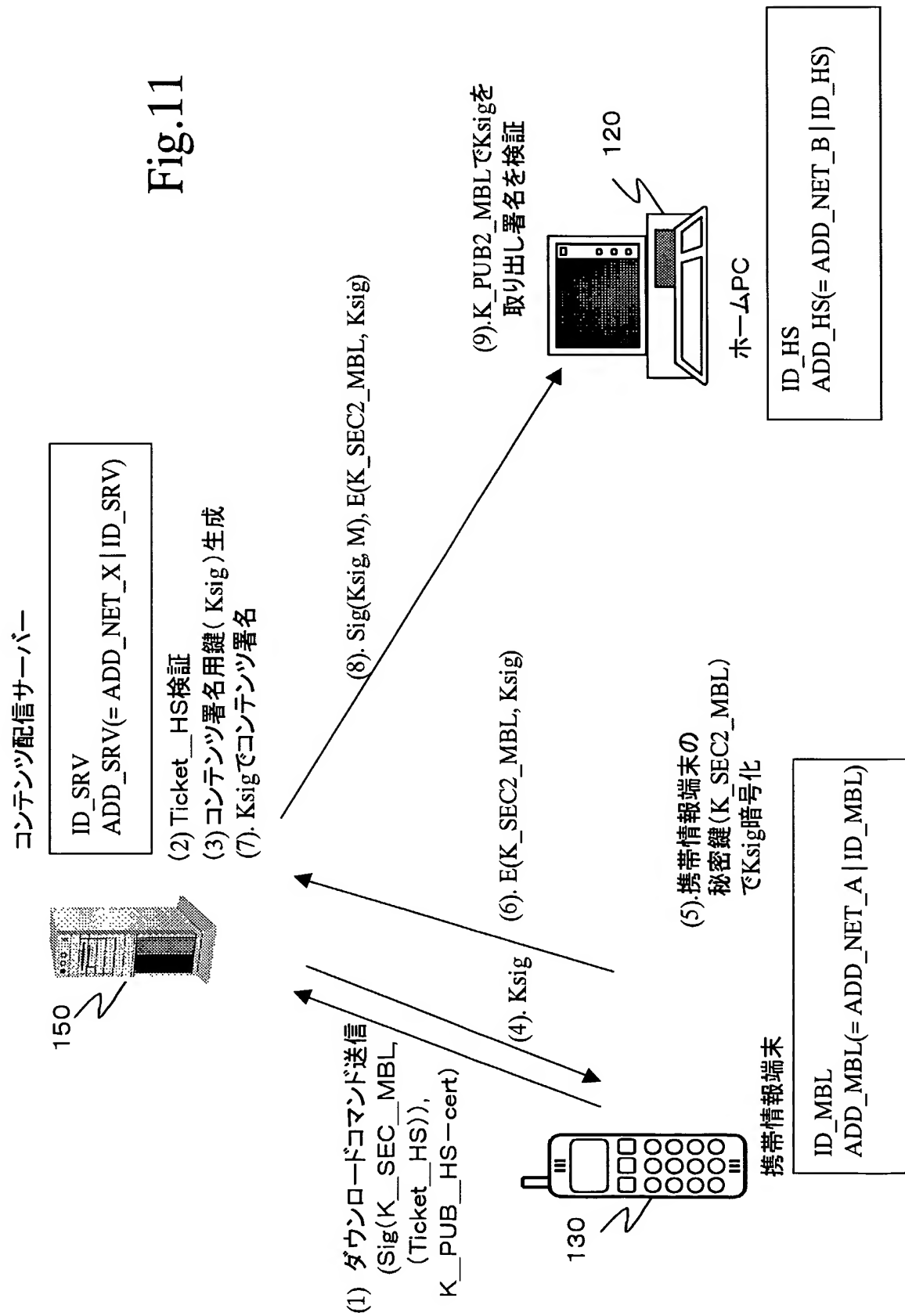


Fig.10

Fig. 11



12/20

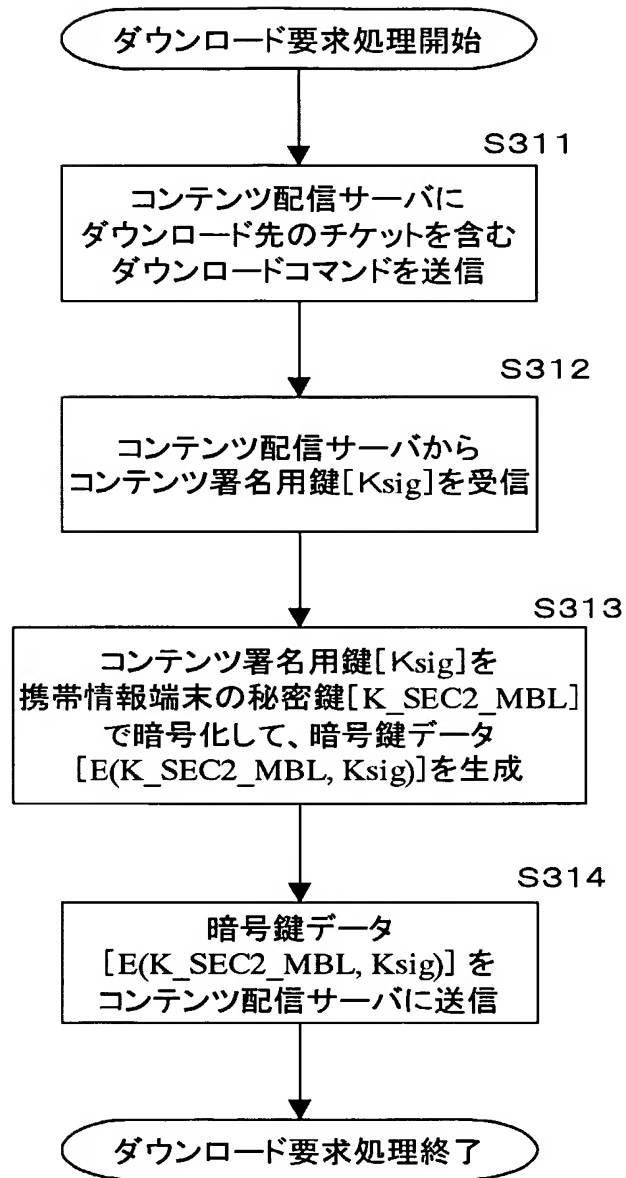
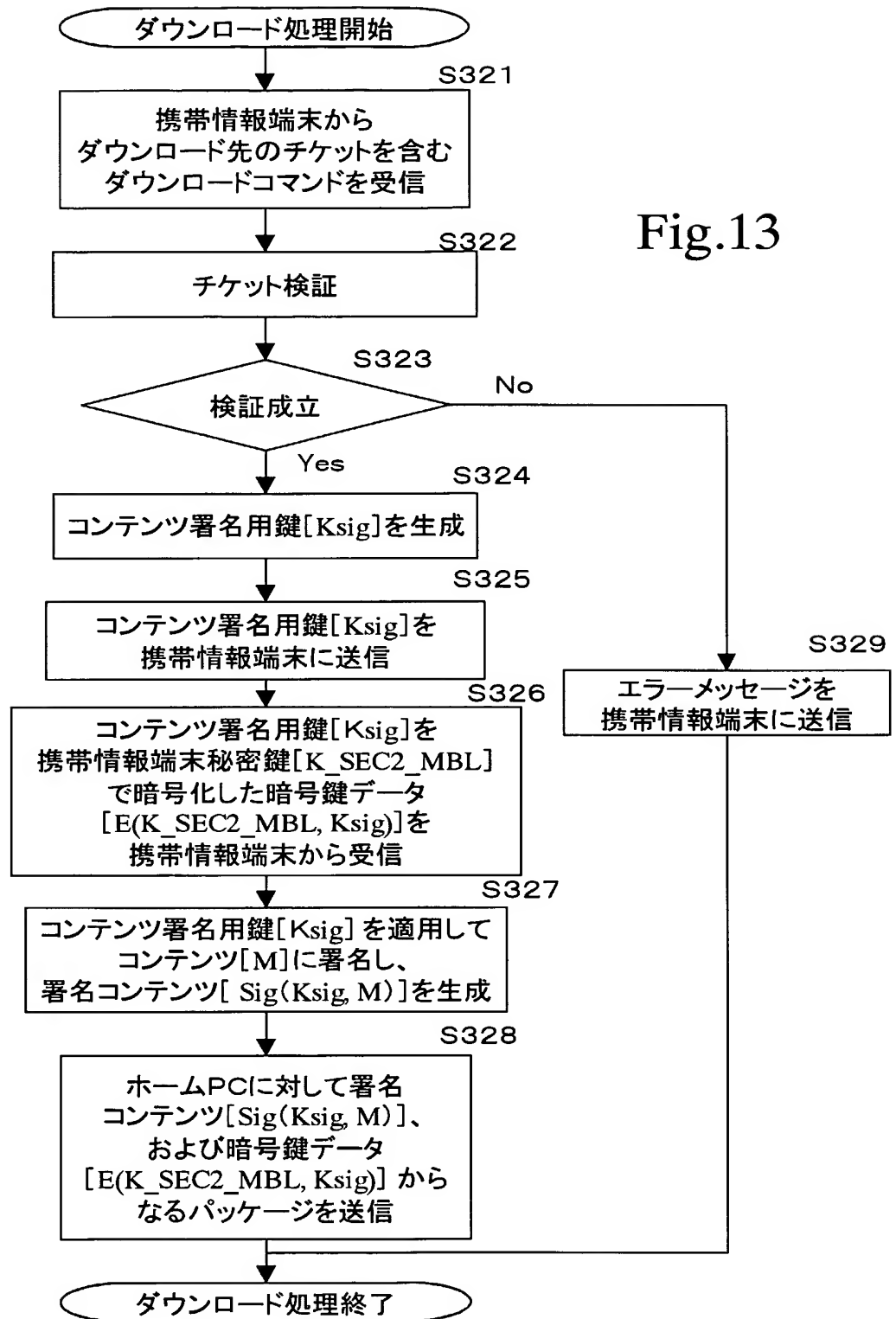


Fig.12

13/20



14/20

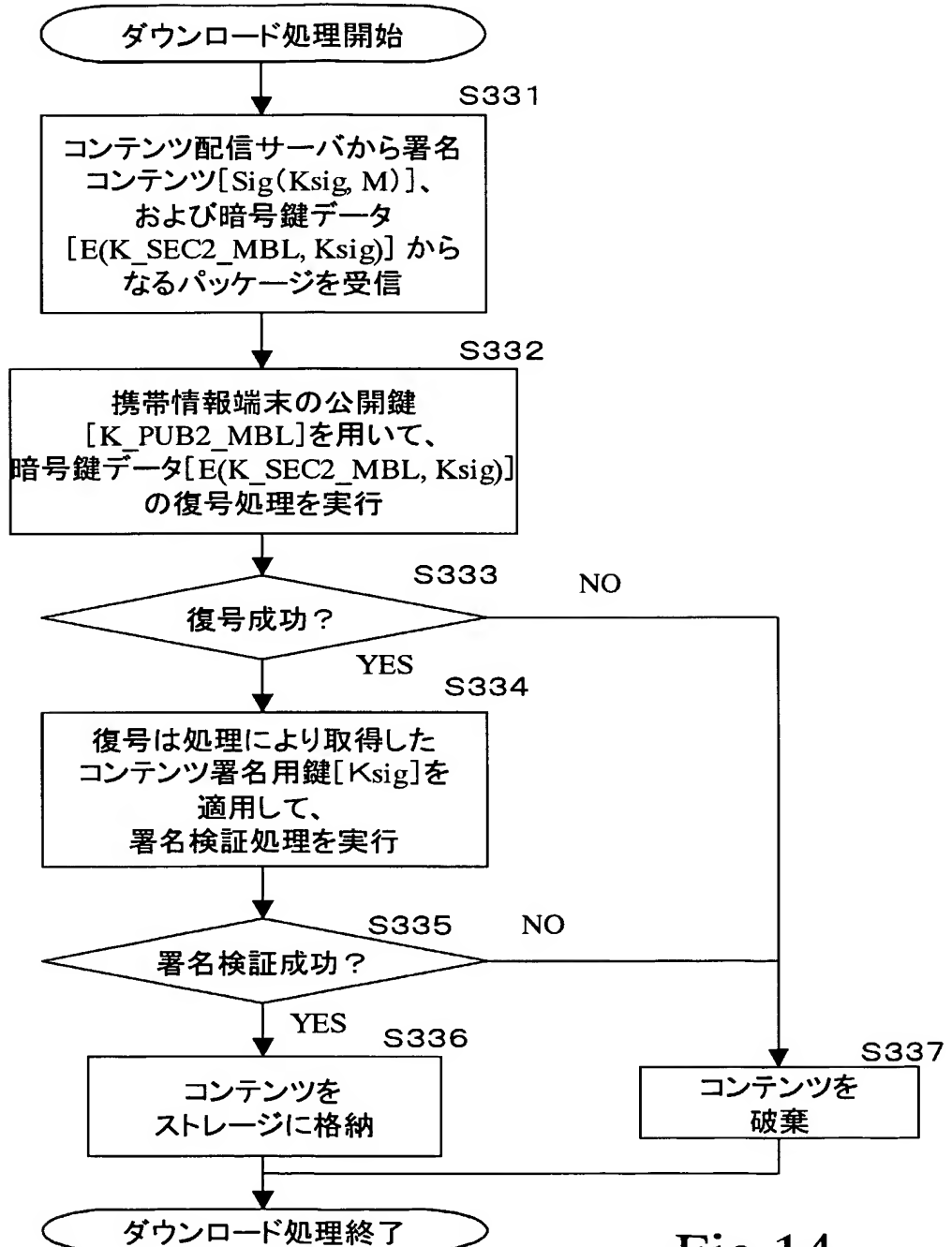
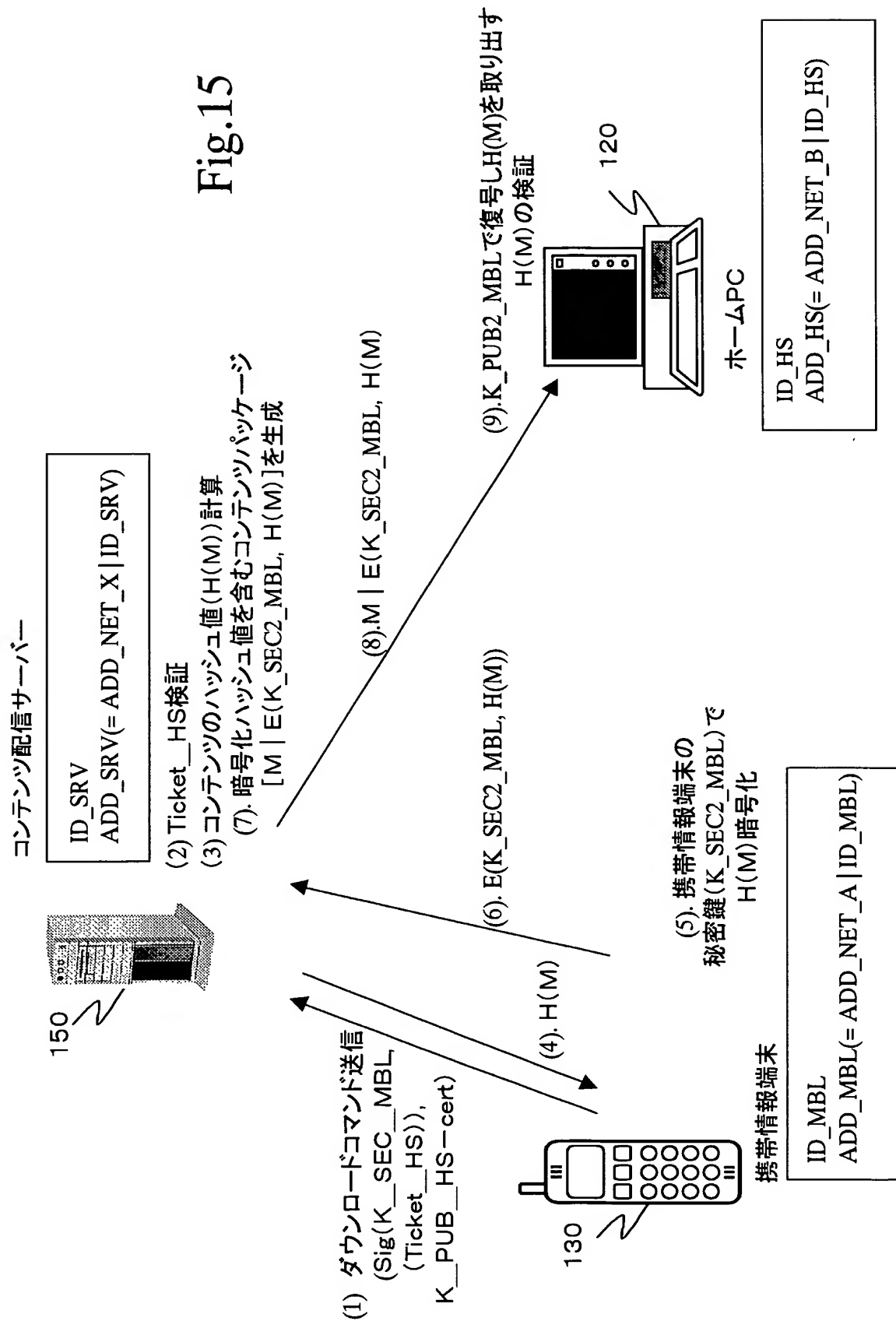


Fig.14

15/20



16/20

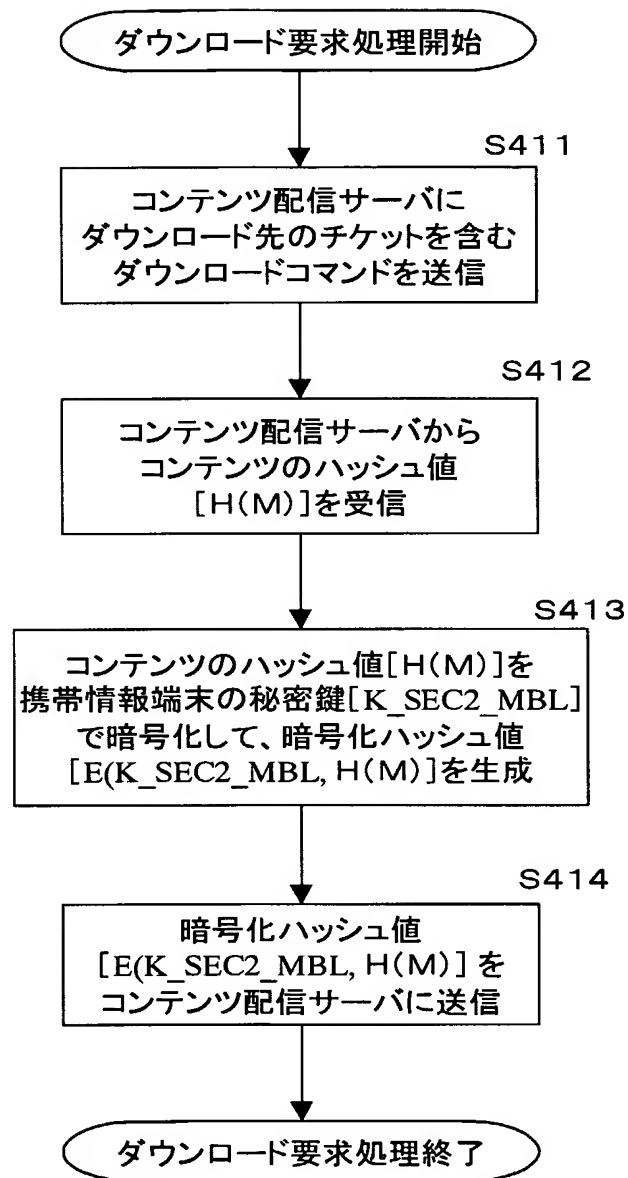


Fig.16

17/20

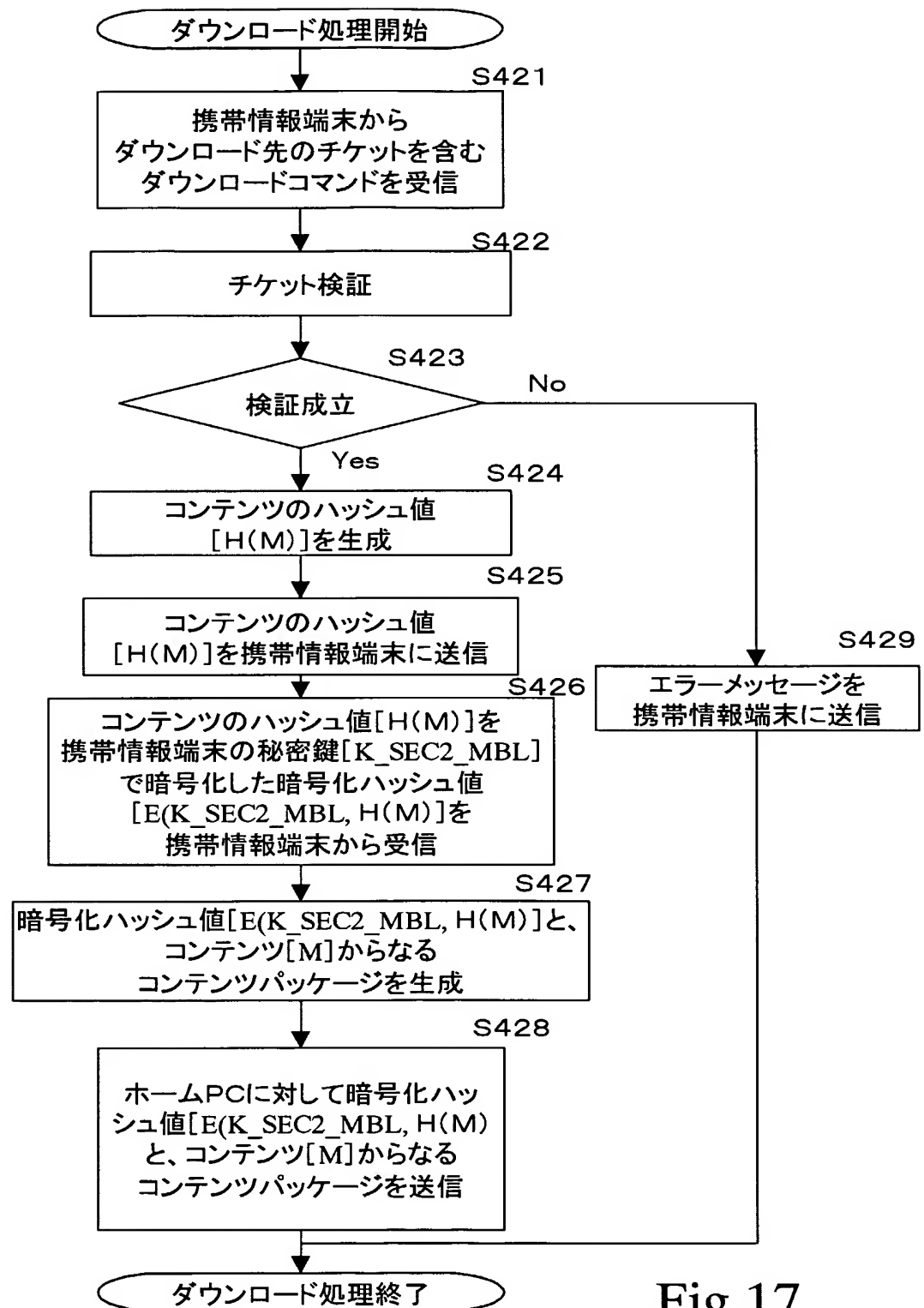


Fig.17

18/20

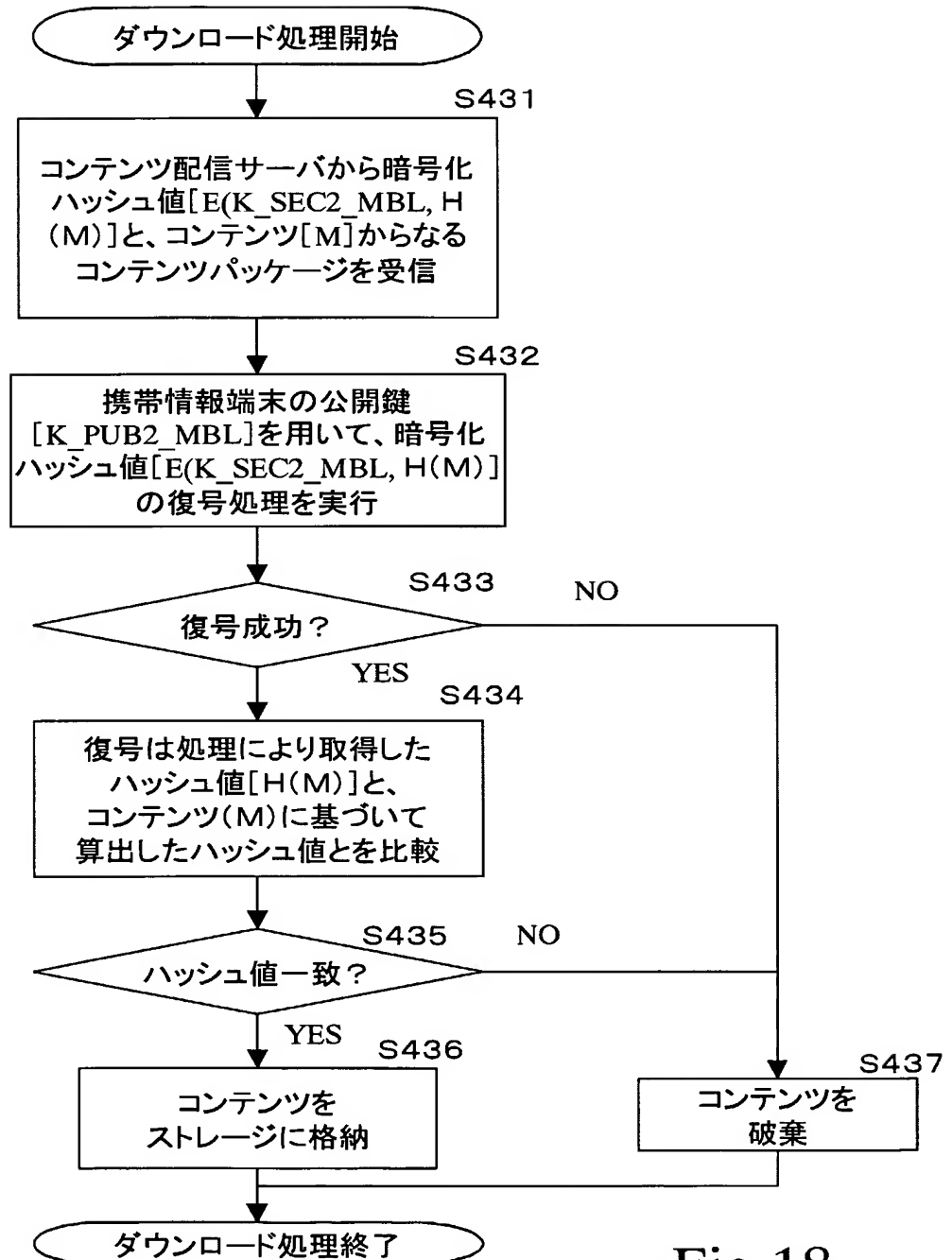
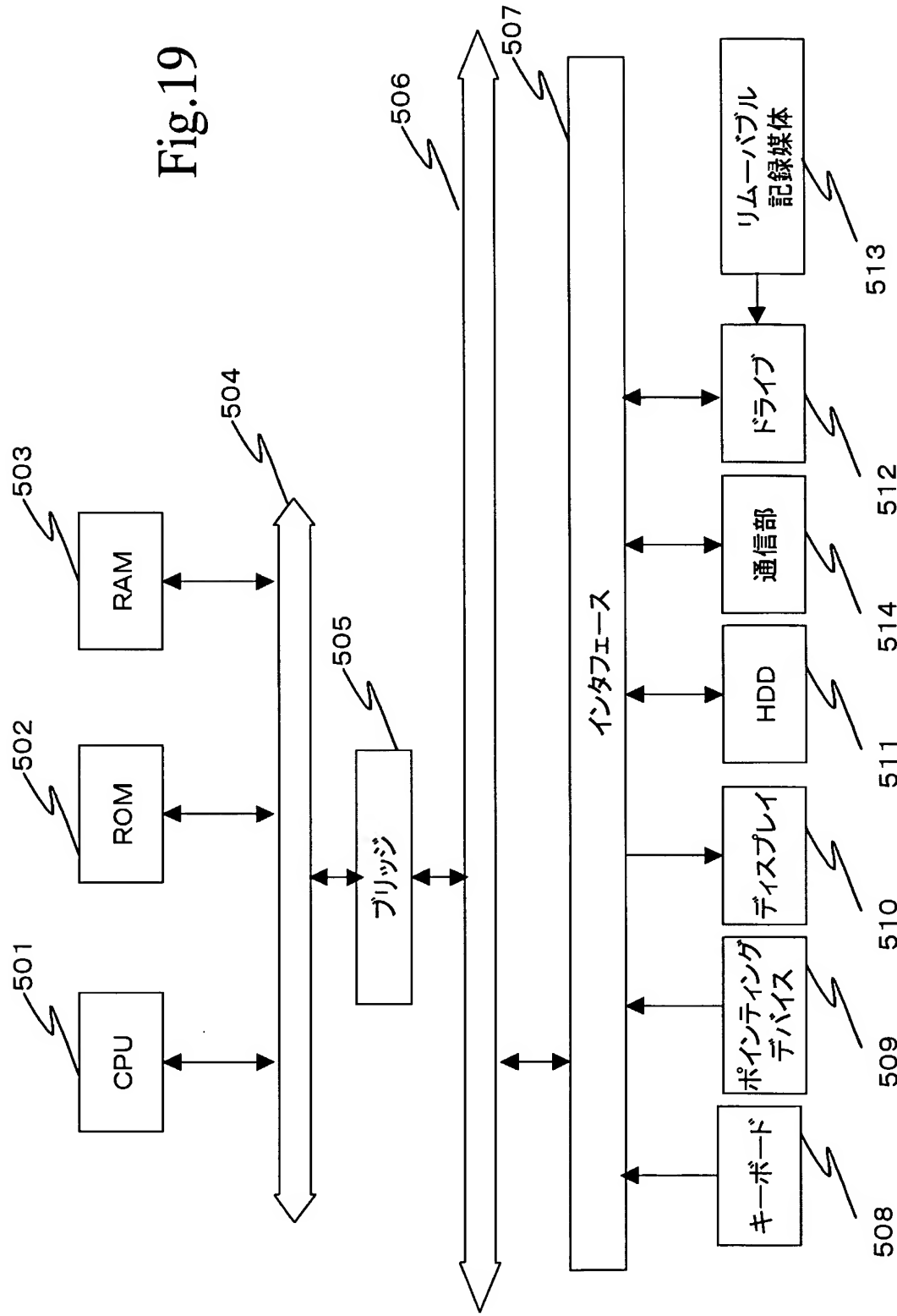


Fig.18

Fig.19



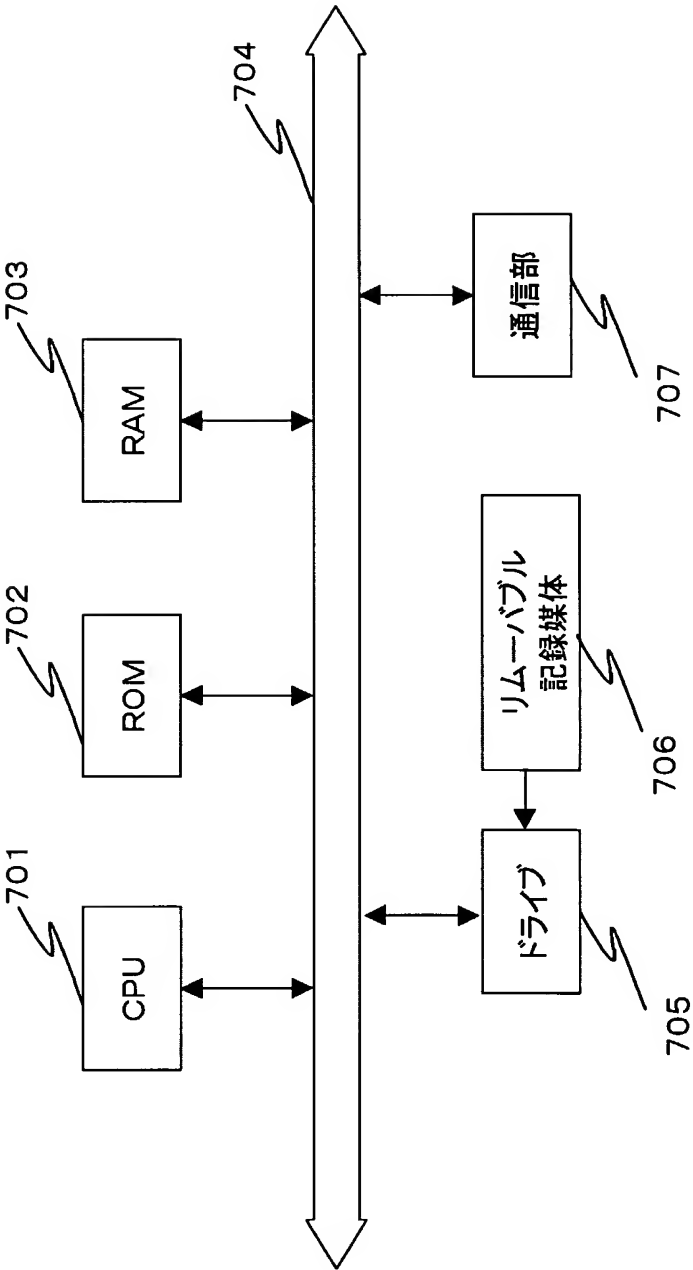


Fig.20

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/00107

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/08, H04L9/32, G06F12/14, G06F15/00, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/08, H04L9/32, G06F12/14, G06F15/00, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-335208 A (Nippon Telegraph And Telephone Corp.), 17 December, 1996 (17.12.96), Full text; Figs. 1 to 21 (Family: none)	1-21
Y	JP 11-174956 A (International Business Machines Corp.), 02 July, 1999 (02.07.99), Par. Nos. [0009] to [0010], [0016] to [0021]; Figs. 1 to 3, 6 & US 6393563 B	1-21

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
07 April, 2003 (07.04.03)

Date of mailing of the international search report
22 April, 2003 (22.04.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/00107

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-285766 A (Matsushita Electric Industrial Co., Ltd.), 12 October, 2001 (12.10.01), Par. Nos. [0060] to [0063]; Fig. 1 (Family: none)	1-21
A	JP 2001-290912 A (NTT Data Corp.), 19 October, 2001 (19.10.01), Par. Nos. [0007], [0036] to [0040] (Family: none)	1-21
P,A	JP 2002-189908 A (Nippon Telegraph And Telephone Corp.), 05 July, 2002 (05.07.02), Full text; Figs. 1 to 30 (Family: none)	1-21

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L9/32, G06F12/14, G06F15/00,
G06F13/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, H04L9/32, G06F12/14, G06F15/00,
G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2003年
日本国登録実用新案公報 1994-2003年
日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 8-335208 A (日本電信電話株式会社) 1996. 12. 17, 全文, 図1-21 (ファミリーなし)	1-21
Y	JP 11-174956 A (インターナショナル・ビジネス・ マシーンズ・コーポレーション) 1999. 07. 02, 第【0009】-【0010】段落, 第【0016】-【0021】段落, 図1-3, 6 & US 6393563 B	1-21

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

07. 04. 03

国際調査報告の発送日

22.04.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳



5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2001-285766 A (松下電器産業株式会社) 2001. 10. 12 第【0060】-【0063】段落, 図1 (ファミリーなし)	1-21
A	J P 2001-290912 A (株式会社エヌ・ティ・ティ・ データ) 2001. 10. 19, 第【0007】段落, 第【0036】-【0040】段落 (ファミリーなし)	1-21
P, A	J P 2002-189908 A (日本電信電話株式会社) 2002. 07. 05, 全文, 図1-30 (ファミリーなし)	1-21